IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

SABLE NETWORKS, INC. AND SABLE IP, LLC, ***Plaintiffs,*** v. **CISCO SYSTEMS, INC.,** ***Defendant.***	**Civil Action No._________** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Sable Networks, Inc. and Sable IP, LLC (collectively, "Sable" or "Plaintiffs") bring this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 6,954,431 (the "'431 patent"); 6,977,932 (the "'932 patent"); 7,012,919 (the "'919 patent"); 7,428,209 (the "'209 patent"); 8,085,775 (the "'775 patent"); and 8,817,790 (the "'790 patent") (collectively, the "patents-in-suit"). Defendant Cisco Systems, Inc. ("Cisco" or "Defendant") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. The patents-in-suit arise from technologies developed by Dr. Lawrence G. Roberts - one of the founding fathers of the internet.[1] The patents relate to technologies for efficiently managing the flow of data packets over routers and switch devices. Dr. Roberts and engineers at

[1] Chris Woodford, THE INTERNET: A HISTORICAL ENCYCLOPEDIA VOLUME 2 at 204 (2005) ("Widely regarded as one of the founding fathers of the Internet, Lawrence Roberts was the primary architect of ARPANET, the predecessor of the Internet.").

Caspian Networks, Inc. and later Sable Networks, Inc. developed these technologies to address the increasing amount of data sent over computer networks.

2. Dr. Roberts is best known for his work as the Chief Scientist of the Advanced Research Projects Agency (ARPA) where he designed and oversaw the implementation of ARPANET, the precursor to the internet. Dr. Roberts' work on ARPANET played a key role in the development of digital network transmission technologies.[2] Initially, ARPANET was used primarily to send electronic mail and Dr. Roberts developed the first program for reading and sending electronic messages.

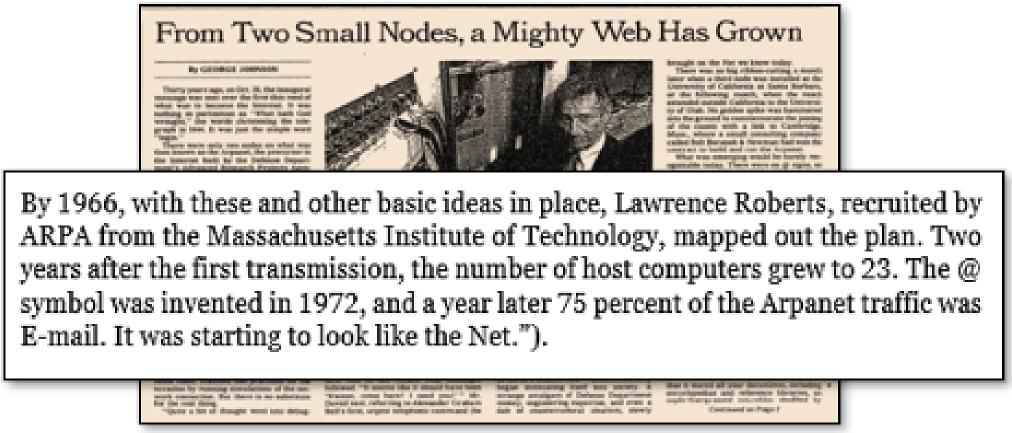
Keenan Mayo and Peter Newcomb, *How The Web Was Won*, VANITY FAIR at 96-97 (January 7, 2009); *One of the Engineers Who Invented the Internet Wants to Build A Radical new Router,* IEEE SPECTRUM MAGAZINE (July 2009); Katie Hafner, *Billions Served Daily, and Counting*, N.Y. TIMES at G1 (December 6, 2001)("Lawrence Roberts, who was then a manager at the Advanced Research Projects Agency's Information Processing Techniques Office, solved that problem after his boss began complaining about the volume of e-mail piling up in his in box. In 1972, Dr. Roberts produced the first e-mail manager, called RD, which included a filing system, as well as a Delete function.").

3. Dr. Roberts' work on ARPANET played a key role in the development of packet switching networks.[3] Packet switching is a digital network transmission process in which data is

[2] Katie Hafner, *Lawrence Roberts, Who Helped Design Internet's Precursor,* N.Y. TIMES at A2 (December 31, 2018) ("Dr. Roberts was considered the decisive force behind packet switching, the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.").

[3] Katie Hafner, *Lawrence Roberts, Who Helped Design Internet's Precursor,* N.Y. TIMES at A2 (December 31, 2018) ("Dr. Roberts was considered the decisive force behind packet switching,

broken into parts which are sent independently and reassembled at a destination. Electronic messages sent over the ARPANET were broken up into packets then routed over a network to a destination. "In designing the ARPANET, Roberts expanded on the work he'd done at MIT, using those tiny data packets to send information from place to place."[4] Packet switching has become the primary technology for data communications over computer networks.



From Two Small Nodes, a Mighty Web Has Grown

By 1966, with these and other basic ideas in place, Lawrence Roberts, recruited by ARPA from the Massachusetts Institute of Technology, mapped out the plan. Two years after the first transmission, the number of host computers grew to 23. The @ symbol was invented in 1972, and a year later 75 percent of the Arpanet traffic was E-mail. It was starting to look like the Net.").

George Johnson, *From Two Small Nodes, a Mighty Web Has Grown*, N.Y. TIMES at F1 (October 12, 1999).

4. After leaving ARPANET, Dr. Roberts grew increasingly concerned that existing technologies for routing data packets were incapable of addressing the increasing amounts of data

the technology that breaks data into discrete bundles that are then sent along various paths around a network and reassembled at their destination.").

[4] Code Metz, *Larry Roberts Calls Himself the Founder of The Internet. Who Are You To Argue*, WIRED MAGAZINE (September 24, 2012); John C. McDonald, FUNDAMENTALS OF DIGITAL SWITCHING at 211 (1990) ("The ARPANET was, in part, an experimental verification of the packet switching concept. Robert's objective was a new capability for resource sharing.").

traversing the internet.[5] Dr. Roberts identified that as the "Net grows, the more loss and transmission of data occurs. Eventually, gridlock will set in."[6]

> ***The Internet is broken. I should know: I designed it***. In 1967, I wrote the first plan for the ancestor of today's Internet, the Advanced Research Projects Agency Network, or ARPANET, and then led the team that designed and built it. The main idea was to share the available network infrastructure by sending data as small, independent packets, which, though they might arrive at different times, would still generally make it to their destinations. The small computers that directed the data traffic-I called them Interface Message Processors, or IMPs-evolved into today's routers, and for a long time they've kept up with the Net's phenomenal growth. Until now.

Lawrence Roberts, *A Radical New Router*, IEEE SPECTRUM Vol. 46(7) at 34 (August 2009) (emphasis added).

5. In 1998, Dr. Roberts founded Caspian Networks.[7] At Caspian Networks, Dr. Roberts developed a new kind of internet router to efficiently route packets over a network. This new router was aimed at addressing concerns about network "gridlock." In a 2001 interview with Wired Magazine, Dr. Roberts discussed the router he was developing at Caspian Networks – the Apeiro. "Roberts says the Apeiro will also create new revenue streams for the carriers by solving the 'voice and video problem.' IP voice and video, unlike email and static Web pages, breaks down dramatically if there's a delay - as little as a few milliseconds - in getting packets from host to recipient."[8]

6. The Apeiro debuted in 2003. The Apeiro, a flow-based router, can identify the nature of a packet – be it audio, text, or video, and prioritize it accordingly. The Apeiro included

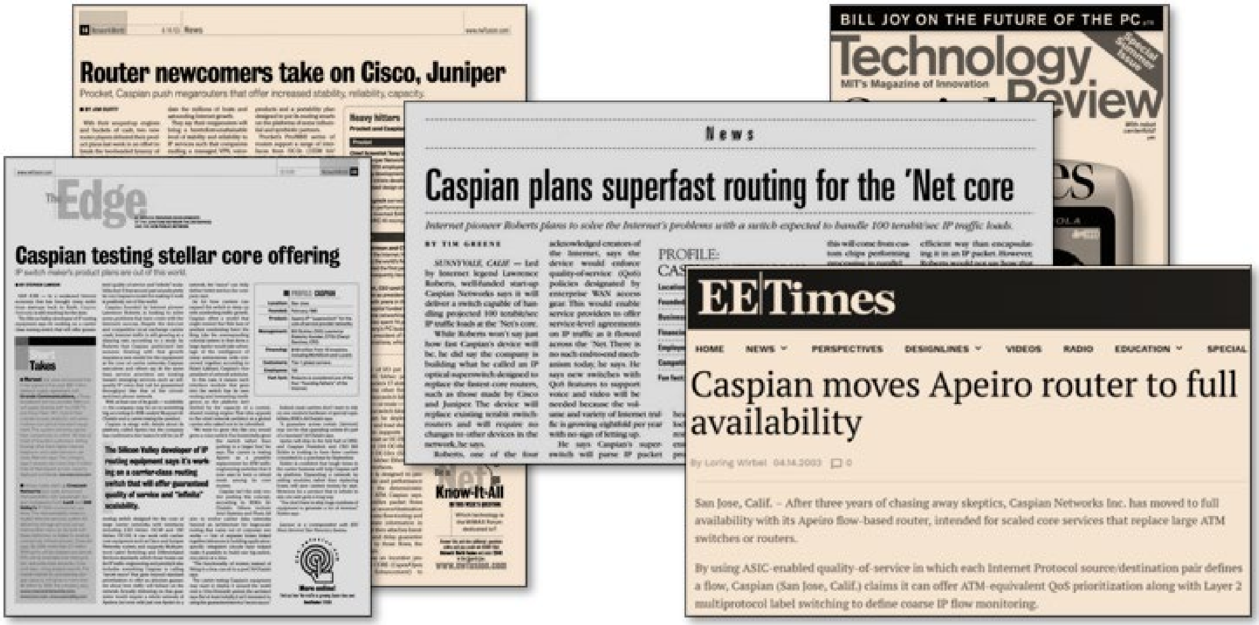
[5] eWeek Editors, *Feeling A Little Congested,* EWEEK MAGAZINE (September 24, 2001) ("Lawrence Roberts, one of the primary developers of Internet precursor ARPANet and CTO of Caspian Networks, recently released research indicating that Net traffic has quadrupled during the past year alone.").

[6] Michael Cooney, *Can ATM Save The Internet,* NETWORK WORLD at 16 (May 20, 1996); Lawrence Roberts, A RADICAL NEW ROUTER, IEEE Spectrum Vol. 46 34-39 (August 2009).

[7] Caspian Networks, Inc. was founded in 1998 as Packetcom, LLC and changed its name to Caspian Networks, Inc. in 1999.

[8] John McHugh, *The n-Dimensional Superswitch*, WIRED MAGAZINE VOL. 9.05 at 88 (May 1, 2001).

numerous technological advances including quality of service (QoS) routing and flow-based routing.


Router newcomers take on Cisco, Juniper

Procket, Caspian push megarouters that offer increased stability, reliability, capacity.

BILL JOY ON THE FUTURE OF THE PC

Technology Review

MIT's Magazine of Innovation

The Edge

Caspian testing stellar core offering

News

Caspian plans superfast routing for the 'Net core

Internet pioneer Roberts plans to solve the Internet's problems with a switch expected to handle 100 terabit/sec IP traffic loads.

BY TIM GREENE

PROFILE:

EE|Times

HOME NEWS PERSPECTIVES DESIGNLINES VIDEOS RADIO EDUCATION SPECIAL

Caspian moves Apeiro router to full availability

By Loring Wirbel 04.14.2003 0

San Jose, Calif. – After three years of chasing away skeptics, Caspian Networks Inc. has moved to full availability with its Apeiro flow-based router, intended for scaled core services that replace large ATM switches or routers.

By using ASIC-enabled quality-of-service in which each Internet Protocol source/destination pair defines a flow, Caspian (San Jose, Calif.) claims it can offer ATM-equivalent QoS prioritization along with Layer 2 multiprotocol label switching to define coarse IP flow monitoring.

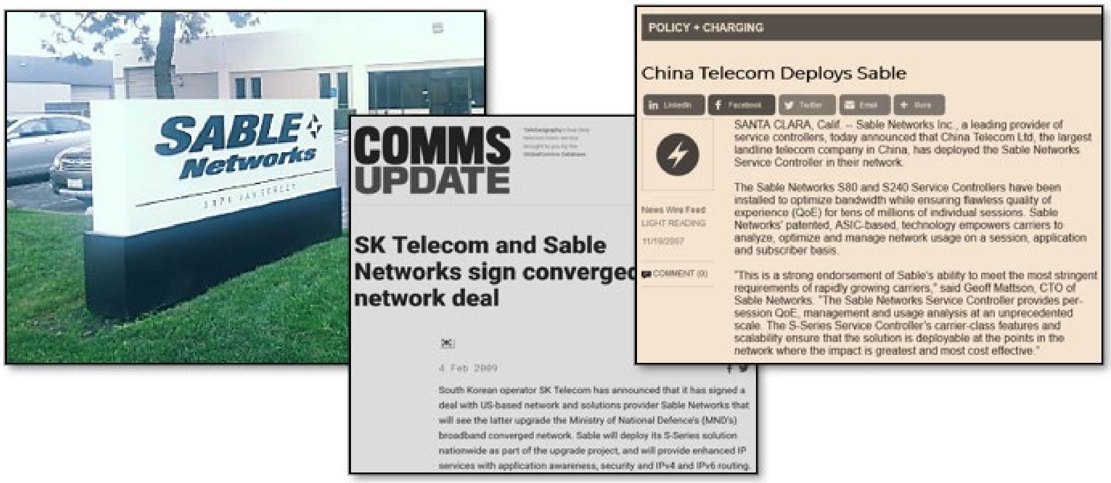
Jim Duffy, *Router Newcomers take on Cisco, Juniper*, NETWORK WORLD at 14 (April 14, 2013); Stephen Lawson, *Caspian Testing Stellar Core Offering*, NETWORK WORLD at 33 (December 17, 2001); Tim Greene, *Caspian Plans Superfast Routing For The 'Net Core*, NETWORK WORLD at 10 (January 29, 2001); Andrew P. Madden, *Company Spotlight: Caspian Networks*, MIT TECHNOLOGY REVIEW at 33 (August 2005); and Loring Wirbel, *Caspian Moves Apeiro Router To Full Availability*, EE TIMES (April 14, 2003).

7. At its height, Caspian Networks Inc. raised more than $300 million dollars and grew to more than 320 employees in the pursuit of developing and commercializing Dr. Roberts' groundbreaking networking technologies, including building flow-based routers that advanced quality of service and load balancing performance. However, despite early success with its technology and business, Caspian hit hard times when the telecommunications bubble burst.

8. Sable Networks, Inc. was formed by Dr. Sang Hwa Lee to further develop and commercialize the flow-based networking technologies developed by Dr. Roberts and Caspian Networks.[9] Sable Networks, Inc. has continued its product development efforts and has gained

[9] Dr. Lee, through his company Mobile Convergence, Ltd. purchased the assets of Caspian Networks Inc. and subsequently created Sable Networks, Inc.

commercial success with customers in Japan, South Korea, and China. Customers of Sable Networks, Inc. have included: SK Telecom, NTT Bizlink, Hanaro Telecom, Dacom Corporation, USEN Corporation, Korea Telecom, China Unicom, China Telecom, and China Tietong.



COMMS UPDATE

SK Telecom and Sable Networks sign converged network deal

4 Feb 2009

South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks that will see the latter upgrade the Ministry of National Defence's (MND's) broadband converged network. Sable will deploy its S-Series solution nationwide as part of the upgrade project, and will provide enhanced IP services with application awareness, security and IPv4 and IPv6 routing.

POLICY + CHARGING

China Telecom Deploys Sable

News Wire Feed
LIGHT READING
11/19/2007

COMMENT (0)

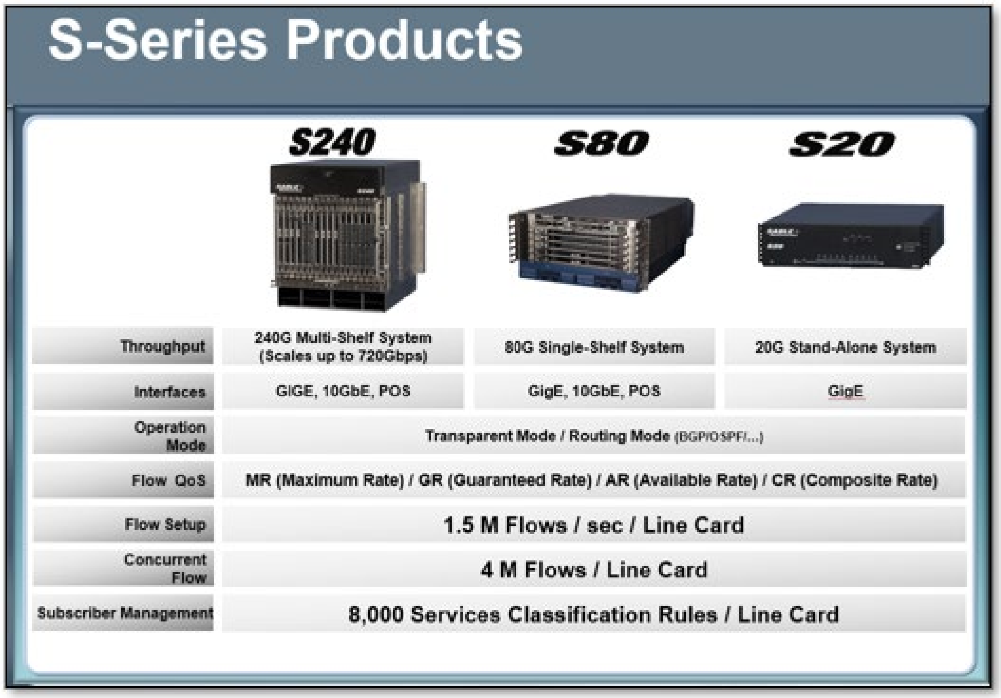
SANTA CLARA, Calif. -- Sable Networks Inc., a leading provider of service controllers, today announced that China Telecom Ltd, the largest landline telecom company in China, has deployed the Sable Networks Service Controller in their network.

The Sable Networks S80 and S240 Service Controllers have been installed to optimize bandwidth while ensuring flawless quality of experience (QoE) for tens of millions of individual sessions. Sable Networks' patented, ASIC-based, technology empowers carriers to analyze, optimize and manage network usage on a session, application and subscriber basis.

"This is a strong endorsement of Sable's ability to meet the most stringent requirements of rapidly growing carriers," said Geoff Mattson, CTO of Sable Networks. "The Sable Networks Service Controller provides per-session QoE, management and usage analysis at an unprecedented scale. The S-Series Service Controller's carrier-class features and scalability ensure that the solution is deployable at the points in the network where the impact is greatest and most cost effective."

SK Telecom and Sable Networks Sign Convergence Network Deal, COMMS UPDATE – TELECOM NEWS SERVICE (February 4, 2009) ("South Korean operator SK Telecom has announced that it has signed a deal with US-based network and solutions provider Sable Networks."); *China Telecom Deploys Sable*, LIGHT READING NEWS FEED (November 19, 2007) ("Sable Networks Inc., a leading provider of service controllers, today announced that China Telecom Ltd, the largest landline telecom company in China, has deployed the Sable Networks Service Controller in their network.").

9. Armed with the assets of Caspian Networks Inc. as well as members of Caspian Networks' technical team, Sable Networks, Inc. continued the product development efforts stemming from Dr. Roberts' flow-based router technologies. Sable Networks, Inc. developed custom application-specific integrated circuits ("ASIC") designed for flow traffic management. Sable Network, Inc.'s ASICs include the Sable Networks SPI, which enables 20 Gigabit flow processing. In addition, Sable Networks, Inc. developed and released S-Series Service Controllers (*e.g.*, S80 and S240 Service Controller models) that contain Sable Networks' flow-based programmable ASICs, POS and Ethernet interfaces, and carrier-hardened routing and scalability from 10 to 800 Gigabits.



S-Series Products

	S240	S80	S20
Throughput	240G Multi-Shelf System (Scales up to 720Gbps)	80G Single-Shelf System	20G Stand-Alone System
Interfaces	GIGE, 10GbE, POS	GigE, 10GbE, POS	GigE
Operation Mode	Transparent Mode / Routing Mode (BGP/OSPF/...)		
Flow QoS	MR (Maximum Rate) / GR (Guaranteed Rate) / AR (Available Rate) / CR (Composite Rate)		
Flow Setup	1.5 M Flows / sec / Line Card		
Concurrent Flow	4 M Flows / Line Card		
Subscriber Management	8,000 Services Classification Rules / Line Card		

SABLE NETWORKS S-SERIES SERVICE CONTROLLERS (showing the S240-240G Multi-Shelf System, S80-80G Single-Shelf System, and S20-20G Stand-Alone System).

10. Sable pursues the reasonable royalties owed for Cisco's use of the inventions claimed in Sable's patent portfolio, which arise from Caspian Networks and Sable Networks' groundbreaking technology.

SABLE'S PATENT PORTFOLIO

11. Sable's patent portfolio includes over 34 patent assets, including 14 granted U.S. patents. Dr. Lawrence Roberts' pioneering work on QoS traffic prioritization, flow-based switching and routing, and the work of Dr. Roberts' colleagues at Caspian Networks Inc. and Sable Networks, Inc. are claimed in the various patents owned by Sable.

12. Highlighting the importance of the patents-in-suit is the fact that the Sable's patent portfolio has been cited by over 1,000 U.S. and international patents and patent applications assigned to a wide variety of the largest companies operating in the computer networking field. Sable's patents have been cited by companies such as:

- ***Cisco Systems, Inc.***[10]
- Juniper Networks, Inc.[11]
- Broadcom Limited[12]
- EMC Corporation[13]
- F5 Networks, Inc.[14]
- Verizon Communications Inc.[15]
- Microsoft Corporation[16]
- Intel Corporation[17]
- Extreme Networks, Inc.[18]
- Huawei Technologies Co., Ltd.[19]

13. The Sable patent portfolio has been cited by Cisco in over 77 of its own patents and patent applications. Over fifteen years after Dr. Roberts developed the technologies that are at issue in this case, Cisco recognized the need to manage the escalating volumes of network data through flow-based handling of data packets. At Cisco's 2020 customer conference, Scott Harrell, senior vice president of Cisco's Internet Based Networking Group, trumpeted Cisco's "brand-new solution" of using data flows in network switches.

> ***It's a brand-new solution*** that actually integrates directly inside of your existing products, ACI, DCNM, and for your data center and allows you to actually use

[10] *See, e.g.*, U.S. Patent Nos. 7,411,965; 7,436,830; 7,539,499; 7,580,351; 7,702,765; 7,817546; 7,936,695; 8,077,721; 8,493,867; 8,868,775; and 9,013,985.

[11] *See, e.g.*, U.S. Patent Nos. 7,463,639; 7,702,810; 7,826,375; 8,593,970; 8,717,889; 8,811,163; 8,811,183; 8,964,556; 9,032,089; 9,065,773; and 9,832,099.

[12] *See, e.g.*, U.S. Patent No. 7,187,687; 7,206,283; 7,266,117; 7,596,139; 7,649,885; 8,014,315; 8,037,399; 8,170,044; 8,194,666; 8,271,859; 8,448,162; 8,493,988; 8,514,716; and 7,657,703.

[13] *See, e.g.*, U.S. Patent Nos. 6,976,134; 7,185,062; 7,404,000; 7,421,509; 7,864,758; and 8,085,794.

[14] *See, e.g.*, U.S. Patent Nos. 7,206,282; 7,580,353; 8,418,233; 8,565,088; 9,225,479; 9,106,606; 9,130,846; 9,210,177; 9,614,772; 9,967,331; and 9,832,069.

[15] *See, e.g.*, U.S. Patent Nos. 7,349,393; 7,821,929; 8,218,569; 8,289,973; 9,282,113; and 8,913,623.

[16] *See, e.g.*, U.S. Patent Nos. 7,567,504; 7,590,736; 7,669,235; 7,778,422; 7,941,309; 7,636,917; 9,571,550; and 9,800,592.

[17] *See, e.g.*, U.S. Patent Nos. 7,177,956; 7,283,464; 9,485,178; 9,047,417; 8,718,096; 8,036,246; 8,493,852; and 8,730,984.

[18] *See, e.g.*, U.S. Patent Nos. 7,903,654; 7,978,614; 8,149839; 10,212,224; 9,112,780; and 8,395,996.

[19] *See, e.g.*, U.S. Patent Nos. 7,903,553; 7,957,421; 10,015,079; 10,505,840; and Chinese Patent Nos. CN108028828 and CN106161333.

> those tools to get to a root cause. And ***we can do things that nobody else can do***. We can actually not only bring out all the stats and the data that we know from your Nexus switches, but we can also combine that with flow data because our cloud-scale ASICs produce the richest set of flow data of any ASICs on the market. And we can use that to quickly pinpoint an issue with an application and get you down to which leaf potentially had a problem, gets you down to whether it was the switch or whether it was the server or whether it was a particular app. ***This is something uniquely that Cisco can do.***

Cisco Live 2020 Opening Keynote, CISCO VIDEO TRANSCRIPTION at 66:12-66:55 (January 27, 2020), *available at*: https://www.youtube.com/watch?v=t-MnUWuC_BU (emphasis added).[20]

THE PARTIES

SABLE NETWORKS, INC.

14. Sable Networks, Inc. ("Sable Networks") is a corporation organized and existing under the laws of the State of California.

15. Sable Networks was formed to continue the research, development, and commercialization work of Caspian Networks Inc., which was founded by Dr. Lawrence Roberts to provide flow-based switching and routing technologies to improve the efficiency and quality of computer networks.

16. Sable Networks is the owner by assignment of all of the patents-in-suit.

SABLE IP, LLC

17. Sable IP, LLC ("Sable IP") is a Delaware limited liability company with its principal place of business at 225 S. 6th Street, Suite 3900, Minneapolis, Minnesota 55402. Pursuant to an exclusive license agreement with Sable Networks, Sable IP is the exclusive licensee of the patents-in-suit.

[20] In 1996, Cisco released a service called NetFlow in 1996 that enabled the capture of network traffic statistics on its routers and switches. However, NetFlow was released as service to "provide network administrators with access to IP flow information from their data networks." NETFLOW SERVICES SOLUTION GUIDE at 2 (July 16, 2001). NetFlow standing alone is a network traffic reporting tool and does not control the flow of packets across a router or switch.

CISCO SYSTEMS, INC.

18. Cisco Systems, Inc. ("Cisco"), is a California corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134. Cisco may be served through its registered agent Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, Texas 78701. Cisco is registered to do business in the State of Texas and has been since at least December 29, 1989.

19. Cisco conducts business operations within the Western District of Texas where it sells, develops, and/or markets its products including facilities at 12515 Research Blvd., Building 3, Austin, Texas 78759, and at 18615 Tuscany Stone, San Antonio, Texas 78258.

JURISDICTION AND VENUE

20. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

21. This Court has personal jurisdiction over Cisco in this action because Cisco has committed acts within the Western District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Cisco would not offend traditional notions of fair play and substantial justice. Defendant Cisco, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Cisco is registered to do business in the State of Texas, has offices and facilities in the State of Texas, and actively directs its activities to customers located in the State of Texas.

22. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Cisco is registered to do business in the State of Texas, has offices in the State of Texas, has transacted business in the Western District of Texas and has committed acts of direct and indirect infringement in the Western District of Texas.

23. Cisco has a regular and established place of business in this District and has committed acts of infringement in this District. Cisco has permanent office locations at 12515 Research Blvd., Building 3, Austin, Texas 78759, and at 18615 Tuscany Stone, San Antonio, Texas 78258, both of which are located within this District. Cisco employs full-time personnel such as sales personnel and engineers in this District, including in Austin, Texas. Cisco has also committed acts of infringement in this District by commercializing, marketing, selling, distributing, testing, and servicing certain Accused Products.

24. This Court has personal jurisdiction over Cisco. Cisco has conducted and does conduct business within the State of Texas. Cisco, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, makes, uses, offers for sale, sells, imports, and/or advertises (including by providing an interactive web page) its products and/or services in the United States and the Western District of Texas and/or contributes to and actively induces its customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of an interactive web page) infringing products and/or services in the United States and the Western District of Texas. Cisco, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of its infringing products and/or services, as described below, into the stream of commerce with the expectation that those products will be purchased and used by customers and/or consumers in the Western District of Texas. These infringing products and/or

services have been and continue to be made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in the Western District of Texas. Cisco has committed acts of patent infringement within the Western District of Texas. Cisco interacts with customers in Texas, including through visits to customer sites in Texas. Through these interactions and visits, Cisco directly infringes the patents-in-suit. Cisco also interacts with customers who sell the Accused Products into Texas, knowing that these customers will sell the Accused Products into Texas, either directly or through intermediaries.

25. Cisco has minimum contacts with this District such that the maintenance of this action within this District would not offend traditional notions of fair play and substantial justice. Thus, the Court therefore has both general and specific personal jurisdiction over Cisco.

THE ASSERTED PATENTS

U.S. PATENT NO. 6,954,431

26. U.S. Patent No. 6,954,431 (the "'431 patent") entitled, *Micro-Flow Management*, was filed on December 6, 2001, and claims priority to April 19, 2000. The '431 patent is subject to a 35 U.S.C. § 154(b) term extension of 722 days. Sable Networks, Inc. is the owner by assignment of the '431 patent. Sable IP is the exclusive licensee of the '431 patent. A true and correct copy of the '431 patent is attached hereto as Exhibit A.

27. The '431 patent discloses novel methods and systems for managing data traffic comprising a plurality of micro-flows through a network.

28. The inventions disclosed in the '431 patent improve the quality of service in data transmissions over a computer network by relying on per micro-flow state information that enables rate and delay variation requirements to be within set quantified levels of service.

29. The '431 patent discloses technologies that speed the rate at which data can effectively travel over a computer network by optimizing packet discarding.

30. The ‘431 patent discloses the use of micro-flow state information to determine the rate of each flow, thus optimizing discards and optimizing the quality of service of data transmission.

31. The ‘431 patent discloses methods and systems that avoid networking system degradation by not overloading network switch buffers.

32. The ‘431 patent discloses a method for managing data traffic through a network that determines a capacity of a buffer containing a micro-flow based on a characteristic.

33. The ‘431 patent discloses a method for managing data traffic through a network that assigns an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

34. The ‘431 patent discloses a method for managing data traffic through a network that delegates a portion of available bandwidth in the network to the micro-flow.

35. The ‘431 patent discloses a method for managing data traffic through a network that uses the buffer for damping jitter associated with the micro-flow.

36. The ‘431 patent has been cited by 103 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘431 patent as relevant prior art:

- ***Cisco Systems, Inc.***
- Juniper Networks, Inc.
- Broadcom Limited
- Intel Corporation
- Sun Microsystems, Inc.
- Oracle Corporation
- Samsung Electronics Co., Ltd.
- Adtran, Inc.
- Time Warner Cable, Inc.
- FSA Technologies, Inc.
- Internap Corporation
- France Telecom

- The Boeing Company
- Wistaria Trading, Ltd.

U.S. PATENT NO. 6,977,932

37. U.S. Patent No. 6,977,932 (the "'932 patent") entitled, *System and Method for Network Tunneling Utilizing Micro-Flow State Information*, was filed on January 16, 2002. The '932 patent is subject to a 35 U.S.C. § 154(b) term extension of 815 days. Sable Networks, Inc. is the owner by assignment of the '932 patent. Sable IP is the exclusive licensee of the '932 patent. A true and correct copy of the '932 patent is attached hereto as Exhibit B.

38. The '932 patent discloses novel methods and apparatuses for utilizing a router capable of network tunneling utilizing flow state information.

39. The inventions disclosed in the '932 patent enable the use of micro-flow state information to improve network tunneling techniques.

40. The inventions disclosed in the '932 patent maintain flow state information for various quality of service characteristics by utilizing aggregate flow blocks.

41. The aggregate flow blocks disclosed in the '932 patent maintain micro-flow block information.

42. The technologies claimed in the '932 patent speed the flow of network traffic over computer networks by avoiding time consuming and processor intensive tasks by combining flow state information with other information such as label switched paths utilization information. This permits the micro-flows associated with an aggregate flow block to all be processed in a similar manner.

43. The technologies disclosed in the '932 patent result in more efficient computer networks by avoiding the processor intensive tasks of searching millions of flow blocks to identify

flow blocks having certain micro-flow characteristics in order to process large numbers of micro-flows.

44. The ‘932 patent discloses a router capable of network tunneling utilizing flow state information containing an aggregate flow block having tunnel specific information for a particular network tunnel.

45. The ‘932 patent discloses a router capable of network tunneling utilizing flow state information containing a flow block having flow state information for a micro-flow, the flow block further including an identifier that associates the flow block with the aggregate flow block.

46. The ‘932 patent discloses a router capable of network tunneling utilizing flow state information wherein the aggregate flow block stores statistics for the particular network tunnel.

47. The ‘932 patent has been cited by 86 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘932 patent as relevant prior art:

- ***Cisco Systems, Inc.***
- Juniper Networks, Inc.
- Avaya, Inc.
- Fujitsu, Ltd.
- Intel Corporation
- Nokia Corporation
- Qualcomm, Inc.
- Sprint Communications Co.
- Telefonaktiebolaget LM Ericsson
- Verizon Communications, Inc.

U.S. PATENT NO. 7,012,919

48. U.S. Patent No. 7,012,919 (the “‘919 patent”) entitled, *Micro-Flow Label Switching*, was filed on December 8, 2000, and claims priority to April 19, 2000. The ‘919 patent is subject to a 35 U.S.C. § 154(b) term extension of 1,069 days. Sable Networks, Inc. is the owner

by assignment of the ‘919 patent. Sable IP is the exclusive licensee of the ‘919 patent. A true and correct copy of the ‘919 patent is attached hereto as Exhibit C.

49. The ‘919 patent claims specific methods and systems for providing aggregate micro-flows.

50. The technologies claimed in the ‘919 patent improve data transmission in computer networks by providing micro-flow based label switched path utilization.

51. The inventions taught in the ‘919 patent achieve improvements in intelligent network traffic engineering protocols by providing load balancing based on the utilization of individual label switched paths.

52. In one embodiment described in the ‘919 patent, a method for providing an aggregate micro-flow having intelligent load balancing is disclosed.

53. In this embodiment, a set of label switched paths is defined for a network domain, and as the network receives a set of data packets, a micro-flow comprising the set of data packets is defined.

54. The ‘919 patent further discloses including a quality of service type in addition to the information included in each data packet.

55. The ‘919 patent teaches selecting a label switched path from the defined set of label switched paths based on the quality of service type of the micro-flow.

56. The ‘919 patent discloses a method for providing aggregate micro-flows that defines a set of label switched paths.

57. The ‘919 patent discloses a method for providing aggregate micro-flows that defines a micro-flow comprising a set of data packets, the micro-flow having a quality of service type.

58. The ‘919 patent discloses a method for providing aggregate micro-flows that selects a particular label switched path from the defined set of label switched paths based on the quality of service type of the micro-flow.

59. The ‘919 patent discloses a method for providing aggregate micro-flows that transmits the micro-flow along the selected label switched path, the micro-flow having an associated forwarding equivalence class, the forwarding equivalence class defining additional transmission constraints for the micro-flow.

60. The ‘919 patent has been cited by 242 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘919 patent family as relevant prior art.

- ***Cisco Systems, Inc.***
- Juniper Networks, Inc.
- Advanced Micro Devices, Inc.
- AT&T, Inc.
- Broadcom, Inc.
- Brocade Communications Systems, Inc.
- Arris Enterprises LLC
- Nicira, Inc.
- Extreme Networks, Inc.
- Fortinet, Inc.
- Foundry Networks, Inc.
- Fujitsu Ltd.
- Intel Corporation
- Huawei Technologies Co., Ltd.
- Hitachi, Ltd.
- Hewlett Packard Enterprise Company
- Marlow Technologies, LLC
- Microsoft Corporation
- ServiceNow, Inc.
- Telefonaktiebolaget LM Ericsson
- Telcordia Technologies, Inc.
- Riverbed Technology, Inc.
- Uber Technologies, Inc.
- The Regents of the University of California
- Verizon Communications, Inc.

U.S. PATENT NO. 7,428,209

61. U.S. Patent No. 7,428,209 (the "'209 patent") entitled, *Network Failure Recovery Mechanism*, was filed on June 12, 2001. The '209 patent is subject to a 35 U.S.C. § 154(b) term extension of 655 days. Sable Networks, Inc. is the owner by assignment of the '209 patent. Sable IP is the exclusive licensee of the '209 patent. A true and correct copy of the '209 patent is attached hereto as Exhibit D.

62. The '209 patent discloses novel methods and systems for implementing within a network router a method for recovering from a failure.

63. The inventions disclosed in the '209 patent enable large-scale computer networks to quickly recover from a component failure.

64. The '209 patent discloses a method implemented on a network router that recovers from a failure.

65. The '209 patent discloses a method implemented on a network router for sending, via a first route, a first set of information from an ingress module to a first egress module for forwarding by the first egress module to a destination external to the router, where a first set of information traverses a path which encompasses at least a portion of the first route.

66. The '209 patent discloses a method implemented on a network router for detecting an external failure beyond the first egress module.

67. The '209 patent discloses a method implemented on a network router for directing a message to the ingress module informing the ingress module of the external failure in response to an external failure.

68. The '209 patent discloses a method implemented on a network router for selecting an alternate egress module capable of forwarding information to a destination in response to an error message.

69. The ‘209 patent discloses a method implemented on a network router for sending, via a second route, a future set of information from the ingress module to the alternate egress module for forwarding to the destination, where the first set of information and the future set of information are both part of a flow.

70. The ‘209 patent discloses a method implemented on a network router for causing other sets of information associated with the flow to be sent from the ingress module to the alternate egress module in response to the message.

71. The ‘209 patent discloses a method implemented on a network router for directing to the ingress module that comprises: (1) identifying the ingress module; (2) accessing a routing table which comprises one or more routes to the ingress module; (3) obtaining a return route from the routing table, wherein the return route directs the message to the ingress module along a different path than that traversed by said first set of information; and (4) sending a message to the ingress module via the return route.

72. The ‘209 patent discloses a method implemented on a network router where the first egress module and the alternate egress module are predetermined, where identifiers associated with the first egress module and the alternate egress module are stored within a flow block associated with the flow. Further, the ’209 patent teaches storing an indication in the flow block that all sets of information associated with the flow are to be sent to the alternate egress module.

73. The ‘209 patent family has been cited by 52 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘209 patent family as relevant prior art:

- ***Cisco Systems, Inc.***
- AT&T, Inc.
- Canon, Inc.
- British Telecommunications Public Limited Co.

- EMC Corporation
- Hewlett Packard Enterprise Company
- Infinera Corporation
- International Business Machines Corporation
- ShoreTel, Inc.
- Nokia Corporation
- Monarch Networking Solutions LLC

U.S. PATENT NO. 8,085,775

74. U.S. Patent No. 8,085,775 (the "'775 patent") entitled, *Identifying Flows Based On Behavior Characteristics And Applying User-Defined Actions*, was filed on July 31, 2006. The '775 patent is subject to a 35 U.S.C. § 154(b) term extension of 467 days. Sable Networks, Inc. is the owner by assignment of the '775 patent. Sable IP is the exclusive licensee of the '775 patent. A true and correct copy of the '775 patent is attached hereto as Exhibit E.

75. The '775 patent discloses novel methods for identifying and handling a single application flow of a plurality of information packets.

76. The inventions disclosed in the '775 patent teach methods of identifying, classifying, and controlling information packet flows based on their observed behavior rather than the content of the data packets.

77. The '775 patent teaches technologies that can effectively identify and control specific types of data traffic despite attempts to conceal the content or type of traffic represented by the data packets.

78. The '775 patent discloses a machine-implemented method for the identification and handling of a single application flow that creates a flow block as the first packet of a flow is processed by a router.

79. The ‘775 patent discloses a machine-implemented method for the identification and handling of a single application flow that utilizes a flow block adapted to store payload-content agnostic behavioral statistics about the flow.

80. The ‘775 patent discloses a machine-implemented method for the identification and handling of a single application flow that updates the flow block with the flow’s payload-content agnostic behavioral statistics as packets belonging to the flow are processed by the router.

81. The ‘775 patent discloses a machine-implemented method for the identification and handling of a single application flow that utilizes a flow incapable of being identified by header information alone.

82. The ‘775 patent discloses a machine-implemented method for the identification and handling of a single application flow that heuristically determines whether at least one user-specified policy is satisfied by the payload-content agnostic behavioral statistics stored in the flow block.

83. The ‘775 patent discloses a machine-implemented method for the identification and handling of a single application flow that includes functionality wherein the payload-content agnostic behavioral statistics for the flow are calculated by the router.

84. The ‘775 patent discloses a machine-implemented method for the identification and handling of a single application flow that includes functionality wherein the payload-content agnostic behavioral statistics reflect the empirical behavior of the flow.

85. The ‘775 patent discloses a machine-implemented method for the identification and handling of a single application flow that includes functionality wherein at least one of the payload-content agnostic behavioral statistics is one of the following characteristics: (1) total byte count accumulated for the flow, (2) flow life duration, (3) average rate of flow, (4) average packet size,

(5) average packet rate, (6) average inter-packet gap, (7) instantaneous flow rate, and (8) moving average flow rate.

86. The ‘775 patent has been cited by 36 patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have all cited the ‘775 patent as relevant prior art:

- ***Cisco Systems, Inc.***
- Calix, Inc.
- British Telecommunications Public Limited Company
- Extreme Networks, Inc.
- Fujitsu Ltd.
- Level 3 Communications, Inc.
- Nokia Corporation
- Sprint Spectrum L.P.
- Solana Networks Inc.
- Taiwan Semiconductor Mfg. Co. Ltd.
- Verizon Communications, Inc.

U.S. PATENT NO. 8,817,790

87. U.S. Patent No. 8,817,790 (the "‘790 patent") entitled, *Identifying Flows Based on Behavior Characteristics and Applying User-Defined Actions*, was filed on September 23, 2011, and claims priority to July 31, 2006. Sable Networks, Inc. is the owner by assignment of the ‘790 patent. Sable IP is the exclusive licensee of the ‘790 patent. A true and correct copy of the ‘790 patent is attached hereto as Exhibit F.

88. The ‘790 patent claims specific methods and devices for handling a flow of information packets.

89. The ‘790 patent discloses methods and systems for efficiently identifying undesirable traffic over data networks.

90. The ‘790 patent teaches technologies that identify traffic not by inspecting the payload of each data packet, but rather by analyzing and classifying the behavior of the data flows to identify undesirable traffic.

91. The ‘790 patent discloses applying a user-specified action associated with a policy applicable to data flows that are designated undesirable.

92. The ‘790 patent discloses a method of handling a flow that processes a flow comprised of two or more information packets having header information in common.

93. The ‘790 patent discloses a method of handling a flow that stores header-independent statistics about the flow in a flow block associated with the flow.

94. The ‘790 patent discloses a method of handling a flow that updates the header-independent statistics in the flow block as each information packet belonging to the flow is processed.

95. The ‘790 patent discloses a method of handling a flow that categorizes the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type.

96. The ‘790 patent discloses a method of handling a flow that performs an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

97. The ‘790 patent family has been cited by 24 United States and international patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘790 patent family as relevant prior art:

- ***Cisco Systems, Inc.***
- Solana Networks, Inc.

- British Telecommunications Public Limited Company
- Level 3 Communications, LLC
- Calix, Inc.
- Nokia Corporation
- Verizon Communications, Inc.
- Sprint Spectrum L.P.
- Hon Hai Precision Industry Co., Ltd.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,954,431

98. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

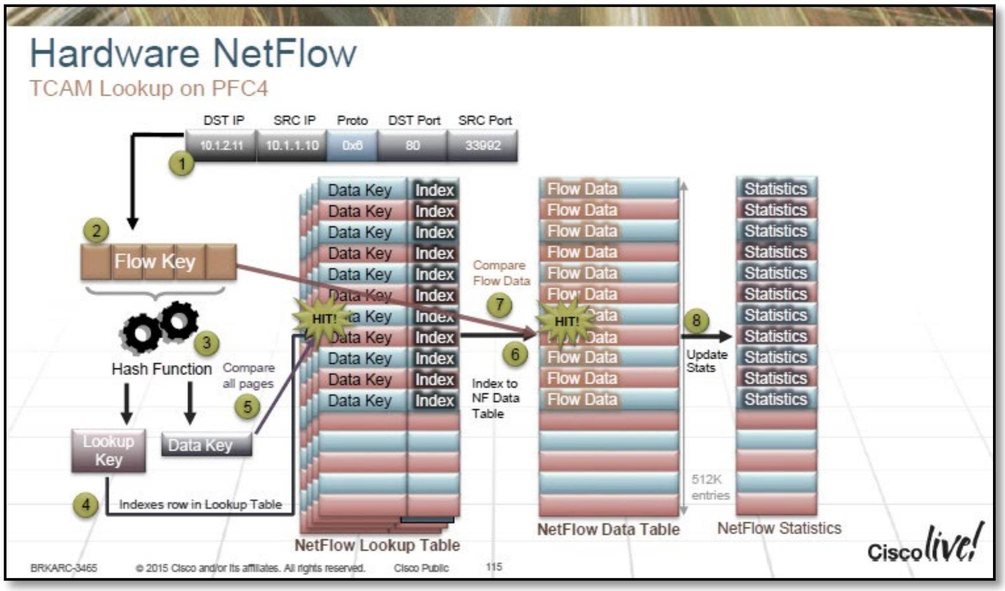
99. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing data traffic comprising a plurality of micro-flows through a network.

100. Cisco designs, makes, sells, offers to sell, imports, and/or uses the following products: Cisco Catalyst 6500 E-Series with Catalyst Supervisor Engine 2T or 2T-XL (including at least models 6503-E, 6504-E, 6506-E, 6509-E, 6509-V-E, and 6513-E); Cisco Catalyst 6800 Series with Supervisor Engine 2T or 2T-XL (including at least model 6807-XL); Cisco Catalyst 7600 Series with Supervisor Engine 2T or 2T-XL (including at least models 7604, 7606-S, 7609-S, and 7613-S); Cisco Catalyst 6500 E-Series with Supervisor Engine 6T (including at least models 6503-E, 6504-E, 6506-E, 6509-E, 6509-V-E, and 6513-E); and Cisco Catalyst 6800 Series with Supervisor Engine 6T (including at least model 6807-XL) (collectively, the "Cisco '431 Products(s)").

101. One or more Cisco subsidiaries and/or affiliates use the Cisco '431 Products in regular business operations.

102. One or more of the Cisco '431 Products include technology for managing data traffic comprising a plurality of micro-flows through a network.

103. The Cisco '431 Products perform a hardware lookup for a microflow of data. The following diagram shows that: (1) the product samples the packet header and (2) generates a "flow key" that is then converted into a hash value that reflects the packet header. The hash value is then compared against the data key in a NetFlow Lookup Table. If the packet matches the values in the NetFlow Data Table, the packet is treated as part of an existing flow. At the same time NetFlow statistics are updated to reflect the incoming packet.



Hardware NetFlow

TCAM Lookup on PFC4

Shawn Wargo, *Catalyst 6800 Switch Architectures*, CISCO LIVE PRESENTATION BRKARC-3465 at 115 (2015).

104. One or more of the Cisco '431 Products determine the capacity of a buffer containing a micro-flow based on a characteristic.

105. One or more of the Cisco '431 Products assign an acceptable threshold value for the capacity of the buffer over a predetermined period of time.

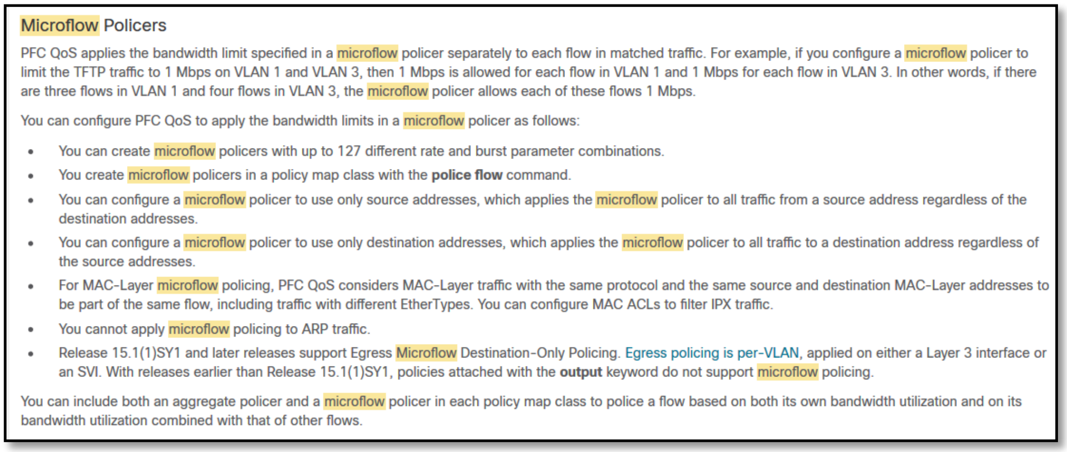
106. One or more of the Cisco '431 Products delegate a portion of available bandwidth in the network to the micro-flow.

107. The Cisco '431 Products enable the setting of thresholds for a buffer that include the ability to set a threshold as a percentage of the buffer.

> For each nonpriority queue, policy-map class queue-buffers or random-detect commands assign QoS values (CoS or DSCP) to thresholds within a queue. Thresholds are configured in numerical order. You cannot skip a threshold, but configuration of all threshold is not required. QoS values that are to be applied to the thresholds must be from the group of values that the class-map filters to the queue.

Release 15.2SY Supervisor Engine 2T Software Configuration Guide, CISCO SUPPORT DOCUMENTATION (February 13, 2019), *available at*: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide.

108. The Cisco '431 Products perform the step of applying a "Microflow Policer" to each flow that matches the flow table values. This process is identified in the following excerpt from Cisco's documentation.



Microflow Policers

PFC QoS applies the bandwidth limit specified in a microflow policer separately to each flow in matched traffic. For example, if you configure a microflow policer to limit the TFTP traffic to 1 Mbps on VLAN 1 and VLAN 3, then 1 Mbps is allowed for each flow in VLAN 1 and 1 Mbps for each flow in VLAN 3. In other words, if there are three flows in VLAN 1 and four flows in VLAN 3, the microflow policer allows each of these flows 1 Mbps.

You can configure PFC QoS to apply the bandwidth limits in a microflow policer as follows:

- You can create microflow policers with up to 127 different rate and burst parameter combinations.
- You create microflow policers in a policy map class with the **police flow** command.
- You can configure a microflow policer to use only source addresses, which applies the microflow policer to all traffic from a source address regardless of the destination addresses.
- You can configure a microflow policer to use only destination addresses, which applies the microflow policer to all traffic to a destination address regardless of the source addresses.
- For MAC-Layer microflow policing, PFC QoS considers MAC-Layer traffic with the same protocol and the same source and destination MAC-Layer addresses to be part of the same flow, including traffic with different EtherTypes. You can configure MAC ACLs to filter IPX traffic.
- You cannot apply microflow policing to ARP traffic.
- Release 15.1(1)SY1 and later releases support Egress Microflow Destination-Only Policing. Egress policing is per-VLAN, applied on either a Layer 3 interface or an SVI. With releases earlier than Release 15.1(1)SY1, policies attached with the **output** keyword do not support microflow policing.

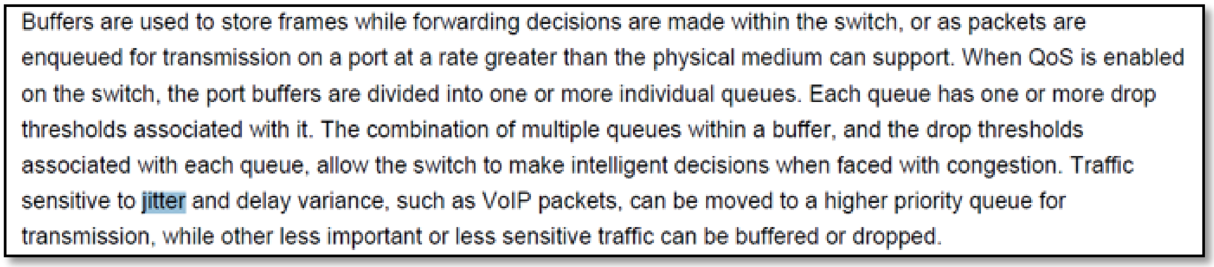
You can include both an aggregate policer and a microflow policer in each policy map class to police a flow based on both its own bandwidth utilization and on its bandwidth utilization combined with that of other flows.

Release 15.2SY Supervisor Engine 2T Software Configuration Guide, CISCO SUPPORT DOCUMENTATION (February 13, 2019) (emphasis added).

109. One or more of the Cisco '431 Products use the buffer for damping jitter associated with the micro-flow. Specifically, the use of queueing allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued. This allow the Cisco' 431 Products to give "delay-sensitive data preferential treatment over other traffic. The switch services traffic in the strict-priority transmit queue before servicing the nonpriority queues. After transmitting a packet from a nonpriority queue, the switch checks for traffic in the strict-priority queue. If the switch detects traffic in the strict-priority queue, it suspends its service of the

nonpriority queue and completes service of all traffic in the strict-priority queue before returning to the nonpriority queue."[21]

110. The Cisco '431 Products use buffers to limit jitter which is delay variance. This process is described in the following excerpt from Cisco's documentation.



Buffers are used to store frames while forwarding decisions are made within the switch, or as packets are enqueued for transmission on a port at a rate greater than the physical medium can support. When QoS is enabled on the switch, the port buffers are divided into one or more individual queues. Each queue has one or more drop thresholds associated with it. The combination of multiple queues within a buffer, and the drop thresholds associated with each queue, allow the switch to make intelligent decisions when faced with congestion. Traffic sensitive to jitter and delay variance, such as VoIP packets, can be moved to a higher priority queue for transmission, while other less important or less sensitive traffic can be buffered or dropped.

Cisco Catalyst 6500/6800 Sup2T System QOS Architecture, Cisco White Paper at 6 (2017) (emphasis added).

111. Cisco has directly infringed and continues to directly infringe the '431 patent by, among other things, making, using, offering for sale, and/or selling technology for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Cisco '431 Products.

112. The Cisco '431 Products are available to businesses and individuals throughout the United States.

113. The Cisco '431 Products are provided to businesses and individuals located in the Western District of Texas.

114. By making, using, testing, offering for sale, and/or selling products and services for managing data traffic comprising a plurality of micro-flows through a network, including but not limited to the Cisco '431 Products, Cisco has injured Plaintiffs and is liable to Plaintiffs for directly

[21] *Release 15.2SY Supervisor Engine 2T Software Configuration Guide,* Cisco Support Documentation (February 13, 2019), *available at*: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide.

infringing one or more claims of the ‘431 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

115. Cisco also indirectly infringes the ‘431 patent by actively inducing infringement under 35 USC § 271(b).

116. Cisco has had knowledge of the ‘431 patent since at least service of this Complaint or shortly thereafter, and Cisco knew of the ‘431 patent and knew of its infringement, including by way of this lawsuit.

117. Alternatively, Cisco has had knowledge of the ‘431 patent since at least August 10, 2010, when U.S. Patent No. 7,773,610, which is owned by Cisco and cites the ‘431 patent as relevant prior art, was issued.

118. Cisco intended to induce patent infringement by third-party customers and users of the Cisco ‘431 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘431 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘431 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco ‘431 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘431 patent, including at least claim 1, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco ‘431 Products to utilize the products in a manner that directly infringe one or more claims of the ‘431 patent.[22] By providing

[22] *See, e.g.,* Shawn Wargo, *Catalyst 6800 Switch Architectures*, CISCO LIVE PRESENTATION BRKARC-3465 (2015); *Release 15.2SY Supervisor Engine 2T Software Configuration Guide,* CISCO SUPPORT DOCUMENTATION (February 13, 2019); SISCO CATALYST 6500/6800 SUP2T SYSTEM QOS ARCHITECTURE WHITE PAPER (2017); *Supervisor Engine 6T Software*

instruction and training to customers and end-users on how to use the Cisco '431 Products in a manner that directly infringes one or more claims of the '431 patent, including at least claim 1, Cisco specifically intended to induce infringement of the '431 patent. Cisco engaged in such inducement to promote the sales of the Cisco '431 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '431 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '431 patent, knowing that such use constitutes infringement of the '431 patent.

119. The '431 patent is well-known within the industry as demonstrated by multiple citations to the '431 patent in published patents and patent applications assigned to technology companies and academic institutions. Cisco is utilizing the technology claimed in the '431 patent without paying a reasonable royalty. Cisco is infringing the '431 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

120. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '431 patent.

121. As a result of Cisco's infringement of the '431 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

Configuration Guide, Release 15.5SY, CISCO SUPPORT DOCUMENTATION (September 2019); *Cisco Catalyst 6500 Series Virtual Switching System*, CISCO WHITE PAPER (December 2012); *Release Notes for Cisco IOS Release 15.1SY,* CISCO DOCUMENTATION (February 19, 2020); *Cisco Catalyst 6800 Series Supervisor Engine 6T Data Sheet,* CISCO DATA SHEET (April 15, 2019); and *Supervisor Engine (Sup6T) Installation,* CISCO YOUTUBE CHANNEL (November 17, 2016), *available at*: https://www.youtube.com/watch?v=4xkfJaQhGuw.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 6,977,932

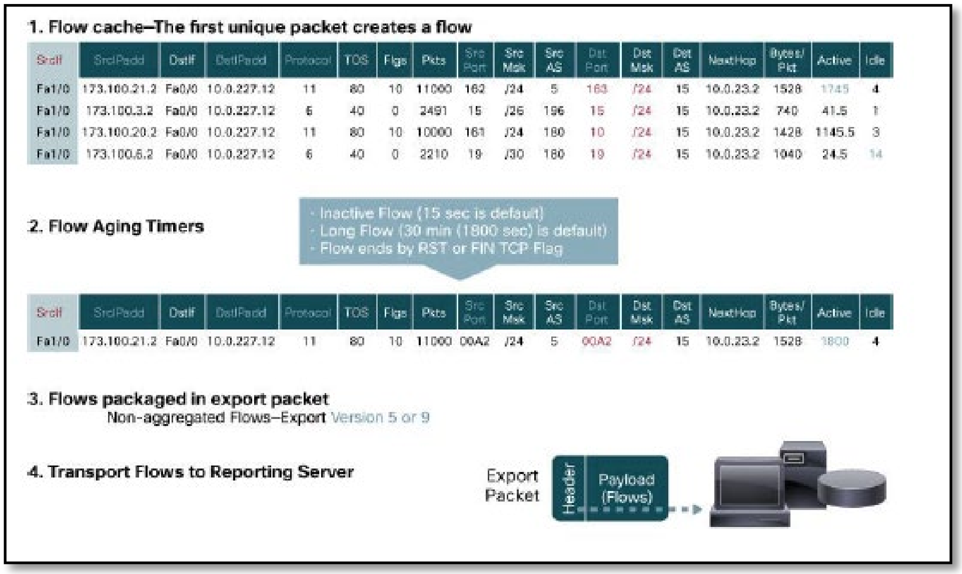
122. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

123. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services utilizing a router capable of network tunneling utilizing flow state information.

124. Cisco designs, makes, sells, offers to sell, imports, and/or uses the following products: Cisco Catalyst 6500 E-Series with Catalyst Supervisor Engine 2T or 2T-XL (including at least models 6503-E, 6504-E, 6506-E, 6509-E, 6509-V-E, and 6513-E); Cisco Catalyst 6800 Series with Supervisor Engine 2T or 2T-XL (including at least model 6807-XL); Cisco Catalyst 7600 Series with Supervisor Engine 2T or 2T-XL (including at least models 7604, 7606-S, 7609-S, and 7613-S); Cisco Catalyst 6500 E-Series with Supervisor Engine 6T (including at least models 6503-E, 6504-E, 6506-E, 6509-E, 6509-V-E, and 6513-E); and the Cisco Catalyst 6800 Series with Supervisor Engine 6T (including at least model 6807-XL) (collectively, the “Cisco '932 Products(s)”).

125. One or more Cisco subsidiaries and/or affiliates use the Cisco ‘932 Products in regular business operations.

126. One or more of the Cisco ‘932 Products perform the step of creating a flow block having flow state information for a receive first data packet on a micro-flow. The below excerpt from Cisco documentation describes that the “first unique packet creates a flow.”



1. Flow cache–The first unique packet creates a flow

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	162	/24	5	163	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	161	/24	180	10	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

2. Flow Aging Timers

- Inactive Flow (15 sec is default)
- Long Flow (30 min (1800 sec) is default)
- Flow ends by RST or FIN TCP Flag

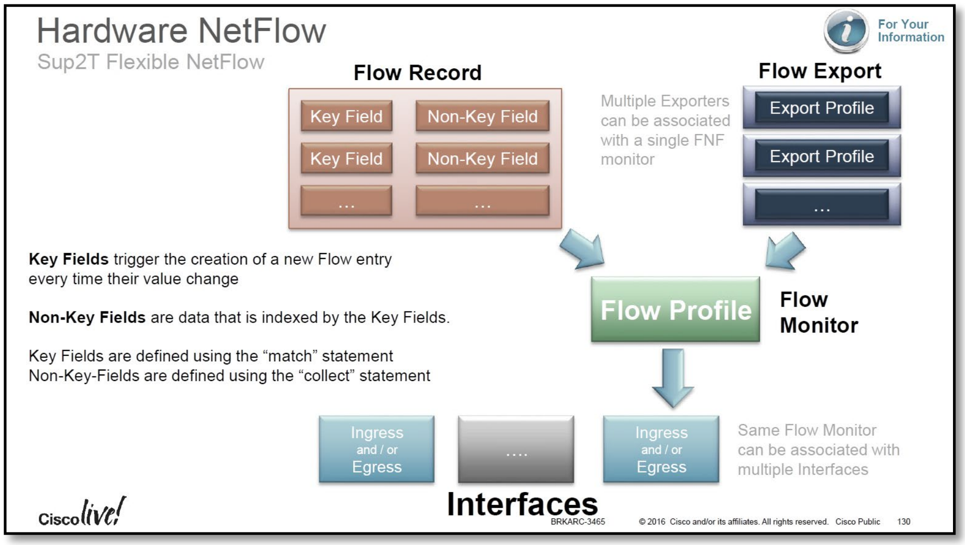
SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Flows packaged in export packet
Non-aggregated Flows–Export Version 5 or 9

4. Transport Flows to Reporting Server

Introduction to Cisco IOS NetFlow, CISCO WHITE PAPER at 5 (May 2012).

127. The Cisco '932 Products further include functionality wherein the receipt of a "Key Field" triggers the creation of a new "Flow Entry" in the "Flow Record." The below excerpt from Cisco's documentation of the '932 Products show the process in which packets from a flow are processed to create a "Flow Entry" in the "Flow Record."



Hardware NetFlow
Sup2T Flexible NetFlow

Key Fields trigger the creation of a new Flow entry every time their value change

Non-Key Fields are data that is indexed by the Key Fields.

Key Fields are defined using the "match" statement
Non-Key-Fields are defined using the "collect" statement

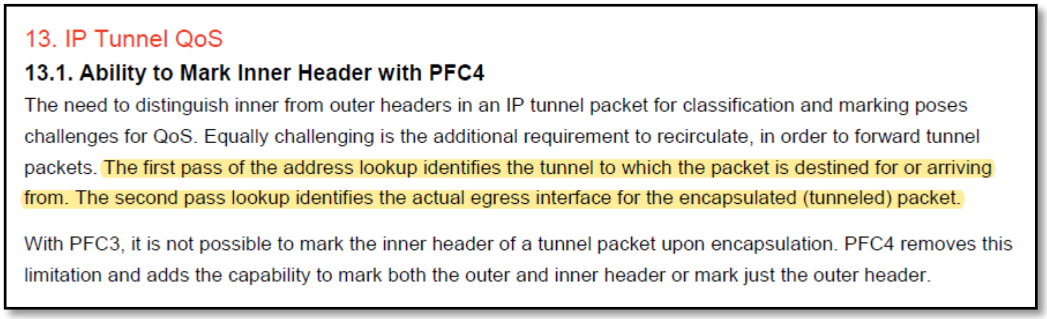
Multiple Exporters can be associated with a single FNF monitor

Same Flow Monitor can be associated with multiple Interfaces

Shawn Wargo, *Catalyst 6800 Switch Architecture,* CISCO PRESENTATION SESSION NO. BRKARC-3465 at 130 (2016) ("Key Fields trigger the creation of a new Flow entry every time their value change").

128. One or more of the Cisco '932 Products include a router capable of network tunneling utilizing flow state information.

129. The Cisco '932 Products include functionality wherein a packet can be identified and the inner and/or outer header can be marked upon encapsulation.



13. IP Tunnel QoS

13.1. Ability to Mark Inner Header with PFC4

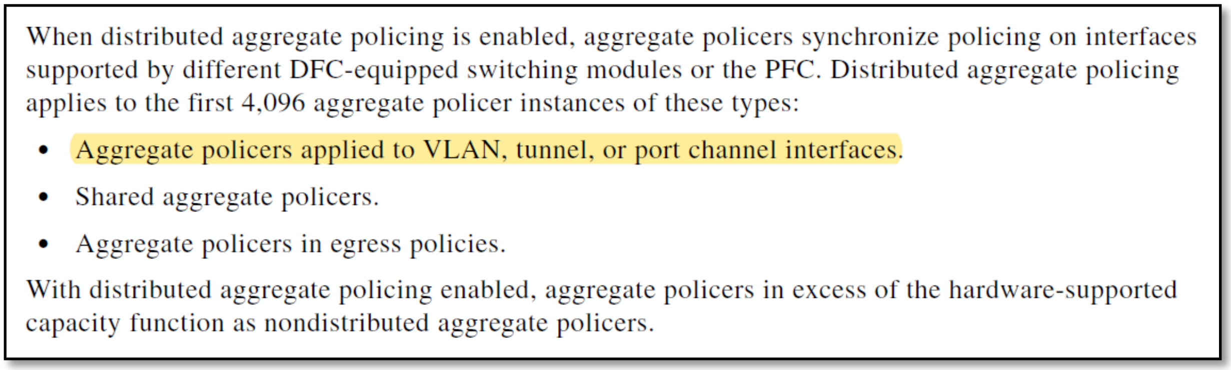
The need to distinguish inner from outer headers in an IP tunnel packet for classification and marking poses challenges for QoS. Equally challenging is the additional requirement to recirculate, in order to forward tunnel packets. The first pass of the address lookup identifies the tunnel to which the packet is destined for or arriving from. The second pass lookup identifies the actual egress interface for the encapsulated (tunneled) packet.

With PFC3, it is not possible to mark the inner header of a tunnel packet upon encapsulation. PFC4 removes this limitation and adds the capability to mark both the outer and inner header or mark just the outer header.

Cisco Catalyst 6500/6800 Sup2T System QOS Architecture, CISCO WHITE PAPER at 21 (2017) (emphasis added).

130. Cisco has directly infringed and continues to directly infringe the '932 patent by, among other things, making, using, offering for sale, and/or selling technology incorporating a router capable of network tunneling utilizing flow state information.

131. One or more of the Cisco '932 Products comprise a router containing an aggregate flow block having tunnel specific information for a particular network tunnel. For example, the Cisco '932 Products support the use of an aggregate policies that have specific information regarding VLAN, tunnels or port interfaces as shown in the below excerpt from Cisco documentation.



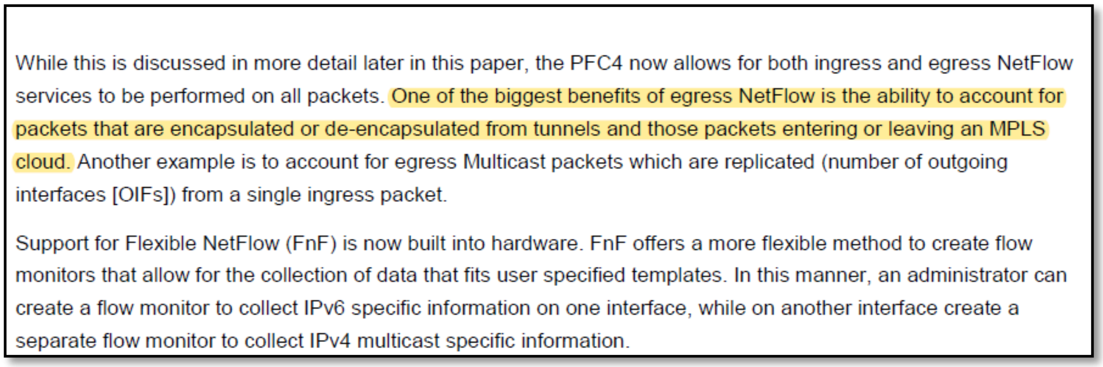
When distributed aggregate policing is enabled, aggregate policers synchronize policing on interfaces supported by different DFC-equipped switching modules or the PFC. Distributed aggregate policing applies to the first 4,096 aggregate policer instances of these types:

- Aggregate policers applied to VLAN, tunnel, or port channel interfaces.
- Shared aggregate policers.
- Aggregate policers in egress policies.

With distributed aggregate policing enabled, aggregate policers in excess of the hardware-supported capacity function as nondistributed aggregate policers.

Supervisor Engine 6T Software Configuration Guide, Release 15.5SY at 25-5 (September 2019) (emphasis added).

132. One or more of the Cisco '932 Products comprise a router containing a flow block having flow state information for a micro-flow, the flow block further including an identifier that associates the flow block with the aggregate flow block. Cisco documentation states that "one of the biggest benefits" is the ability "to account for packets that are encapsulated or de-encapsulated from tunnels."



While this is discussed in more detail later in this paper, the PFC4 now allows for both ingress and egress NetFlow services to be performed on all packets. One of the biggest benefits of egress NetFlow is the ability to account for packets that are encapsulated or de-encapsulated from tunnels and those packets entering or leaving an MPLS cloud. Another example is to account for egress Multicast packets which are replicated (number of outgoing interfaces [OIFs]) from a single ingress packet.

Support for Flexible NetFlow (FnF) is now built into hardware. FnF offers a more flexible method to create flow monitors that allow for the collection of data that fits user specified templates. In this manner, an administrator can create a flow monitor to collect IPv6 specific information on one interface, while on another interface create a separate flow monitor to collect IPv4 multicast specific information.

Cisco Catalyst 6500 Supervisor 2T Architecture, Cisco Whitepaper at 28 (2011) (emphasis added).

133. One or more of the Cisco '932 Products comprise a router wherein the aggregate flow block stores statistics for the particular network tunnel.

134. The Cisco '932 Products are available to businesses and individuals throughout the United States.

135. The Cisco '932 Products are provided to businesses and individuals located in the Western District of Texas.

136. By making, using, testing, offering for sale, and/or selling products utilizing a router capable of network tunneling utilizing flow state information, including but not limited to the Cisco '932 Products, Cisco has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '932 patent, including at least claim 9 pursuant to 35 U.S.C. § 271(a).

137. Cisco also indirectly infringes the '932 patent by actively inducing infringement under 35 USC § 271(b).

138. Cisco has had knowledge of the '932 patent since at least service of this Complaint or shortly thereafter, and Cisco knew of the '932 patent and knew of its infringement, including by way of this lawsuit.

139. Alternatively, Cisco has had knowledge of the '932 patent since at least July 20, 2010, based on its citation of the '932 patent as relevant prior art in three patents that are assigned to and owned by Cisco. These patents include:

- U.S. Patent No. 7,760,636 (assigned to Cisco and issued on July 20, 2010).
- U.S. Patent No. 8,077,721 (assigned to Cisco and issued on December 13, 2011).
- U.S. Patent No. 8,493,867 (assigned to Cisco and issued on July 23, 2013).

140. Cisco intended to induce patent infringement by third-party customers and users of the Cisco '932 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the '932 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '932 patent and with the knowledge that

the induced acts would constitute infringement. For example, Cisco provides the Cisco '932 Products that have the capability of operating in a manner that infringe one or more of the claims of the '932 patent, including at least claim 9, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '932 Products to utilize the products in a manner that directly infringe one or more claims of the '932 patent.[23] By providing instruction and training to customers and end-users on how to use the Cisco '932 Products in a manner that directly infringes one or more claims of the '932 patent, including at least claim 9, Cisco specifically intended to induce infringement of the '932 patent. Cisco engaged in such inducement to promote the sales of the Cisco '932 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '932 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '932 patent, knowing that such use constitutes infringement of the '932 patent.

141. The '932 patent is well-known within the industry as demonstrated by multiple citations to the '932 patent in published patents and patent applications assigned to technology companies and academic institutions. Cisco is utilizing the technology claimed in the '932 patent without paying a reasonable royalty. Cisco is infringing the '932 patent in a manner best described

[23] *See, e.g., Introduction to Cisco IOS NetFlow*, CISCO WHITE PAPER (May 2012); *Cisco Catalyst 6500 Supervisor 2T Architecture,* Cisco Whitepaper (2011); Shawn Wargo, *Catalyst 6800 Switch Architectures*, CISCO LIVE PRESENTATION BRKARC-3465 (2015); *Release 15.2SY Supervisor Engine 2T Software Configuration Guide,* CISCO SUPPORT DOCUMENTATION (February 13, 2019); SISCO CATALYST 6500/6800 SUP2T SYSTEM QOS ARCHITECTURE WHITE PAPER (2017); *Supervisor Engine 6T Software Configuration Guide, Release 15.5SY,* CISCO SUPPORT DOCUMENTATION (September 2019); *Cisco Catalyst 6500 Series Virtual Switching System*, CISCO WHITE PAPER (December 2012); *Release Notes for Cisco IOS Release 15.1SY,* CISCO DOCUMENTATION (February 19, 2020); and *Cisco Catalyst 6800 Series Supervisor Engine 6T Data Sheet,* CISCO DATA SHEET (April 15, 2019).

as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

142. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘932 patent.

143. As a result of Cisco’s infringement of the ‘932 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Cisco’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,012,919

144. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

145. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for providing an aggregate micro-flow.

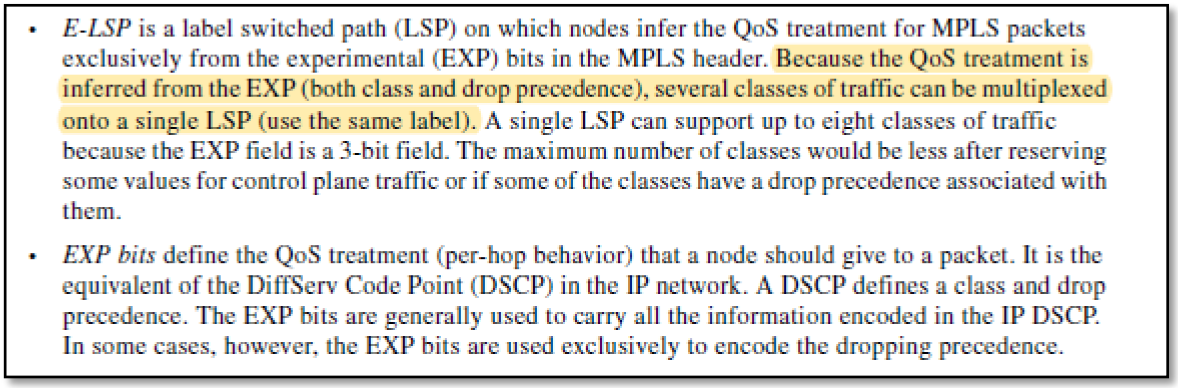
146. Cisco designs, makes, sells, offers to sell, imports, and/or uses the following products: Cisco ASR 9000 Series Aggregation Service Routers (including at least the following models ASR 9001, ASR 9006, ASR 9010, ASR 9901, ASR 9904, ASR 9906, ASR 9910, ASR 9912, and ASR 9922) running the following Cisco IOS XR Software (XR 5.1.x, XR 5.2.x, XR 5.3.x, XR 6.0.x, XR 6.1.x, XR 6.2.x, XR 6.3.x, XR 6.4.x, XR 6.5.x, XR 6.6.x, XR 6.7.x, XR 7.0.x, and XR 7.1.x); Cisco Catalyst 6500 E-Series with Catalyst Supervisor Engine 2T or 2T-XL (including at least the following models 6503-E, 6504-E, 6506-E, 6509-E, 6509-V-E, and 6513-E); Cisco Catalyst 6800 Series with Supervisor Engine 2T or 2T-XL (including at least model 6807-XL); Cisco Catalyst 7600 Series with Supervisor Engine 2T or 2T-XL (including at least models 7604, 7606-S, 7609-S, and 7613-S); Cisco Catalyst 6500 E-Series with Supervisor Engine

6T (including at least models 6503-E, 6504-E, 6506-E, 6509-E, 6509-V-E, and 6513-E); and the Cisco Catalyst 6800 Series with Supervisor Engine 6T (including at least model 6807-XL) (collectively, the "Cisco '919 Products(s)").

147. One or more Cisco subsidiaries and/or affiliates use the Cisco '919 Products in regular business operations.

148. One or more of the Cisco '919 Products include technology for providing an aggregate micro-flow.

149. One or more of the Cisco '919 Products define a set of label switched paths ("LSP"). Specifically, an LSP results from a sequence of hops (Router 0...Router n) through which a packet travels from R0 to Rn by means of label switching mechanisms. A label-switched path can be determined dynamically (based on normal routing mechanisms), or it can be defined explicitly.



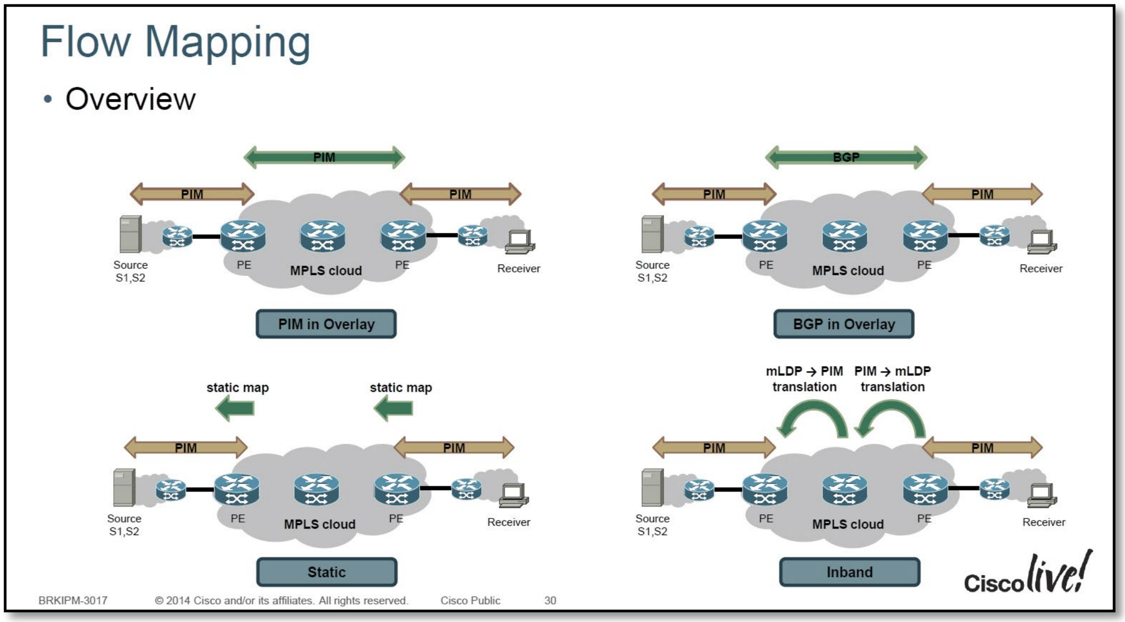
- *E-LSP* is a label switched path (LSP) on which nodes infer the QoS treatment for MPLS packets exclusively from the experimental (EXP) bits in the MPLS header. Because the QoS treatment is inferred from the EXP (both class and drop precedence), several classes of traffic can be multiplexed onto a single LSP (use the same label). A single LSP can support up to eight classes of traffic because the EXP field is a 3-bit field. The maximum number of classes would be less after reserving some values for control plane traffic or if some of the classes have a drop precedence associated with them.
- *EXP bits* define the QoS treatment (per-hop behavior) that a node should give to a packet. It is the equivalent of the DiffServ Code Point (DSCP) in the IP network. A DSCP defines a class and drop precedence. The EXP bits are generally used to carry all the information encoded in the IP DSCP. In some cases, however, the EXP bits are used exclusively to encode the dropping precedence.

CISCO IOS SOFTWARE CONFIGURATION GUIDE, RELEASE 15.0SY: MPLS QOS at 1-2 (January 19, 2018) (emphasis added).

150. One or more of the Cisco '919 Products define a micro-flow comprising a set of data packets, the micro-flow having a quality of service type.

151. One or more of the Cisco '919 Products select a particular label switched path from the defined set of label switched paths based on the quality of service type of the micro-flow. For example, the Cisco '919 Products use Multiprotocol Label Switching ("MPLS"*)* to forward

packets over ethernet. The Cisco '919 Products use label switching in which labels are assigned to packets based on groupings or forwarding equivalence classes ("FEC(s)"). The Cisco '919 Products perform a QoS TCAM lookup on incoming data packets. The results of each QoS TCAM lookup yield an index that contains policer configuration and policing counters. Incoming labels can be aggregate or nonaggregate. An aggregate label indicates that the arriving MPLS or MPLS VPN packet is required to be switched through an IP lookup to find the next hop and the outgoing interface that will be used. A nonaggregate label indicates that the packet already contains the IP next hop information. The label switched paths are stored by the Cisco '919 Products and then assigned to specific flows using one of the following protocols.



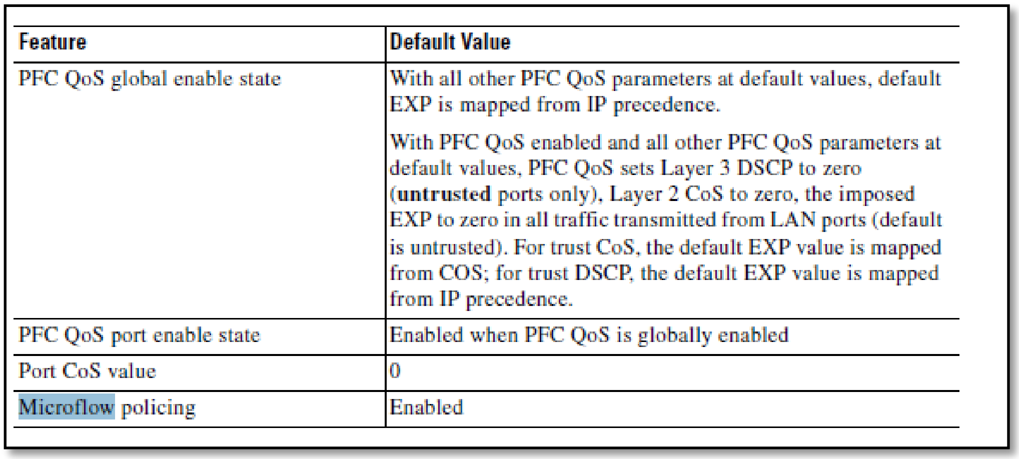
Flow Mapping

- Overview

BRKIPM-3017 © 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public 30

IJsbrand Wijnands and Luc De Ghein, *mVPN Deployment Models*, CISCO LIVE PRESENTATION: BRKIPM-3017 at 30 (2014).

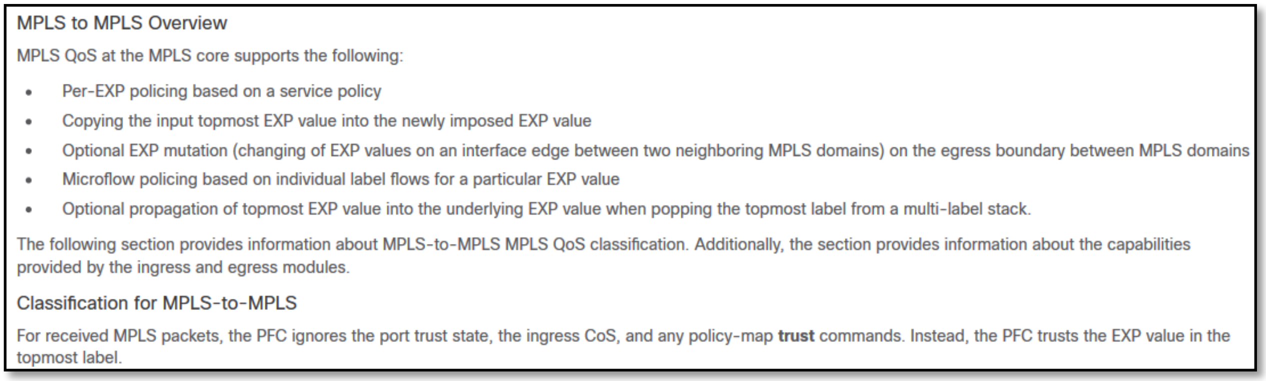
152. One or more of the Cisco '919 Products transmits the micro-flow along the selected label switched path, the micro-flow having an associated forwarding equivalence class, the forwarding equivalence class defining additional transmission constraints for the micro-flow.



Feature	Default Value
PFC QoS global enable state	With all other PFC QoS parameters at default values, default EXP is mapped from IP precedence. With PFC QoS enabled and all other PFC QoS parameters at default values, PFC QoS sets Layer 3 DSCP to zero (**untrusted** ports only), Layer 2 CoS to zero, the imposed EXP to zero in all traffic transmitted from LAN ports (default is untrusted). For trust CoS, the default EXP value is mapped from COS; for trust DSCP, the default EXP value is mapped from IP precedence.
PFC QoS port enable state	Enabled when PFC QoS is globally enabled
Port CoS value	0
Microflow policing	Enabled

SUPERVISOR ENGINE 2T SOFTWARE CONFIGURATION GUIDE, RELEASE 15.4SY at 69-13 (March 2019) (emphasis added) ("With PFC QoS enabled and all other PFC QoS parameters at default values, PFC QoS sets Layer 3 DSCP to zero (untrusted ports only), Layer 2 CoS to zero, the imposed EXP to zero in all traffic transmitted from LAN ports (default is untrusted.").

153. The Cisco '919 Products perform the operation of defining a micro-flow comprising a set of data packets, the micro-flow having a quality of service type. For example, the Cisco '919 Products support "Microflow policing based on individual label flows for a particular EXP value."



MPLS to MPLS Overview

MPLS QoS at the MPLS core supports the following:

- Per-EXP policing based on a service policy
- Copying the input topmost EXP value into the newly imposed EXP value
- Optional EXP mutation (changing of EXP values on an interface edge between two neighboring MPLS domains) on the egress boundary between MPLS domains
- Microflow policing based on individual label flows for a particular EXP value
- Optional propagation of topmost EXP value into the underlying EXP value when popping the topmost label from a multi-label stack.

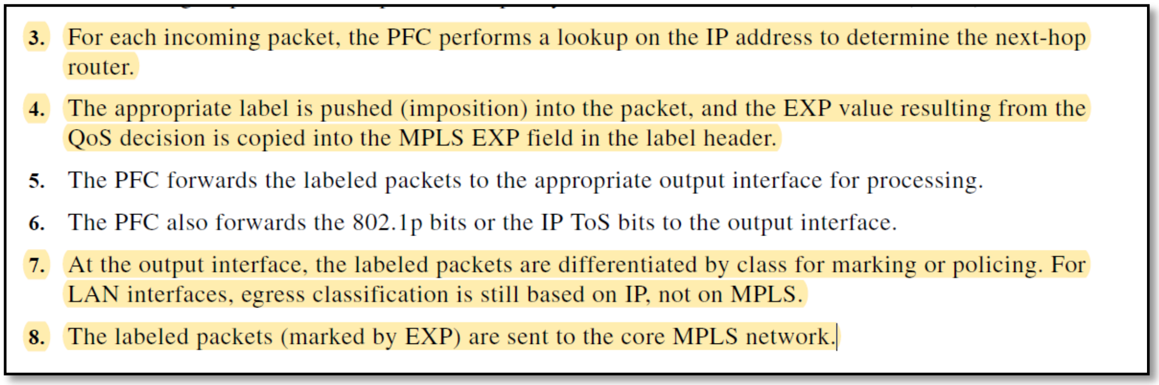
The following section provides information about MPLS-to-MPLS MPLS QoS classification. Additionally, the section provides information about the capabilities provided by the ingress and egress modules.

Classification for MPLS-to-MPLS

For received MPLS packets, the PFC ignores the port trust state, the ingress CoS, and any policy-map **trust** commands. Instead, the PFC trusts the EXP value in the topmost label.

RELEASE 15.3SY SUPERVISOR ENGINE 6T SOFTWARE CONFIGURATION GUIDE – MPLS QOS (March 19, 2019), *available at*:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-3SY/config_guide/

154. Further for each packet that is incoming the packet is assigned to a flow based on the header information (EXP) value resulting from the quality of service decision. The EXP value is then copied into the MPLS EXP field in the label header.



3. For each incoming packet, the PFC performs a lookup on the IP address to determine the next-hop router.
4. The appropriate label is pushed (imposition) into the packet, and the EXP value resulting from the QoS decision is copied into the MPLS EXP field in the label header.
5. The PFC forwards the labeled packets to the appropriate output interface for processing.
6. The PFC also forwards the 802.1p bits or the IP ToS bits to the output interface.
7. At the output interface, the labeled packets are differentiated by class for marking or policing. For LAN interfaces, egress classification is still based on IP, not on MPLS.
8. The labeled packets (marked by EXP) are sent to the core MPLS network.

CISCO IOS SOFTWARE CONFIGURATION GUIDE, RELEASE 15.0SY at 1-6 (2018) (emphasis added).

155. The Cisco '919 Products are available to businesses and individuals throughout the United States.

156. The Cisco '919 Products are provided to businesses and individuals located in the Western District of Texas.

157. Cisco has directly infringed and continues to directly infringe the '919 patent by, among other things, making, using, offering for sale, and/or selling technology for providing an aggregate micro-flow, including but not limited to the Cisco '919 Products.

158. By making, using, testing, offering for sale, and/or selling products and services, including but not limited to the Cisco '919 Products, Cisco has injured Plaintiffs and is liable for directly infringing one or more claims of the '919 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

159. Cisco also indirectly infringes the '919 patent by actively inducing infringement under 35 USC § 271(b).

160. Cisco has had knowledge of the '919 patent since at least service of this Complaint or shortly thereafter, and Cisco knew of the '919 patent and knew of its infringement, including by way of this lawsuit.

161. Alternatively, Cisco has had knowledge of the ‘919 patent since at least August 12, 2008, based on its citation of the ‘919 patent as relevant prior art in four patents that are assigned to and owned by Cisco. These patents include:

- U.S. Patent No. 7,411,965 (assigned to Cisco and issued on August 12, 2008).
- U.S. Patent No. 7,580,351 (assigned to Cisco and issued on August 25, 2009).
- U.S. Patent No. 8,868,775 (assigned to Cisco and issued on October 21, 2014).
- U.S. Patent No. 9,013,985 (assigned to Cisco and issued on April 21, 2015).

162. Cisco intended to induce patent infringement by third-party customers and users of the Cisco ‘919 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘919 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘919 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco ‘919 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘919 patent, including at least claim 1, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco ‘919 Products to utilize the products in a manner that directly infringe one or more claims of the ‘919 patent.[24] By providing

[24] *See, e.g.,* IJsbrand Wijnands and Luc De Ghein, *mVPN Deployment Models*, CISCO LIVE PRESENTATION: BRKIPM-3017 (2014); SUPERVISOR ENGINE 2T SOFTWARE CONFIGURATION GUIDE, RELEASE 15.4SY 69-13 (March 2019); RELEASE 15.3SY SUPERVISOR ENGINE 6T SOFTWARE CONFIGURATION GUIDE – MPLS QOS (March 19, 2019), *available at*: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-3SY/config_guide/sup6T/15_3_sy_swcg_6T/mplsqos.html; Sabyasachi Kar & Shashi Shekhar Sharma, *Next Generation Multicast VPN & Advanced Design,* CISCO LIVE PRESENTATION LTRMPL-3103 (2017); CISCO ASR 9000 SERIES AGGREGATION SERVICES ROUTER MPLS CONFIGURATION GUIDE, RELEASE 5.3.X (August 1, 2015); CISCO ASR 9000 SERIES AGGREGATION SERVICES ROUTER ROUTING CONFIGURATION GUIDE, RELEASE 6.1.X (November 2, 2016); MPLS CONFIGURATION GUIDE FOR CISCO ASR 9000 SERIES ROUTERS, IOS XR RELEASE 6.5.X (September 30, 2019); *ASR 9000 Operation & Troubleshooting,* CISCO LIVE PRESENTATION TECSPG-3001 (2015); CISCO IOS SOFTWARE CONFIGURATION GUIDE,

instruction and training to customers and end-users on how to use the Cisco '919 Products in a manner that directly infringes one or more claims of the '919 patent, including at least claim 1, Cisco specifically intended to induce infringement of the '919 patent. Cisco engaged in such inducement to promote the sales of the Cisco '919 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '919 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '919 patent, knowing that such use constitutes infringement of the '919 patent.

163. The '919 patent is well-known within the industry as demonstrated by multiple citations to the '919 patent in published patents and patent applications assigned to technology companies and academic institutions. Cisco is utilizing the technology claimed in the '919 patent without paying a reasonable royalty. Cisco is infringing the '919 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

164. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '919 patent.

165. As a result of Cisco's infringement of the '919 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

RELEASE 15.0SY: MPLS QOS (January 19, 2018); *Cisco Tech Talk: Traffic Flow Comparison Between Full-Tunnel and Split-Tunnel Modes in PPTP VPN*, CISCO YOUTUBE.COM CHANNEL (last visited April 2020), *available at*: https://www.youtube.com/watch?v=MyjRZ-y5Tco; and *Cisco QoS: Design and Best Practices for Enterprise Networks*, YOUTUBE.COM WEBSITE (December 16, 2013), *available at*: https://www.youtube.com/watch?v=xePZcobaJUY (presented by Ken Briley technical lead at Cisco).

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,428,209

166. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

167. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for implementing within a network router a method for recovering from a failure.

168. Cisco designs, makes, sells, offers to sell, imports, and/or uses Cisco ASR 9000 Series Aggregation Services Routers (including at least models ASR 9001, ASR 9006, ASR 9010, ASR 9901, ASR 9904, ASR 9906, ASR 9910, ASR 9912, and ASR 9922) (collectively, the "Cisco '209 Product(s)").

169. One or more Cisco subsidiaries and/or affiliates use the Cisco ‘209 Products in regular business operations.

170. One or more of the Cisco ‘209 Products include technology for implementing within a network router a method for recovering from a failure.

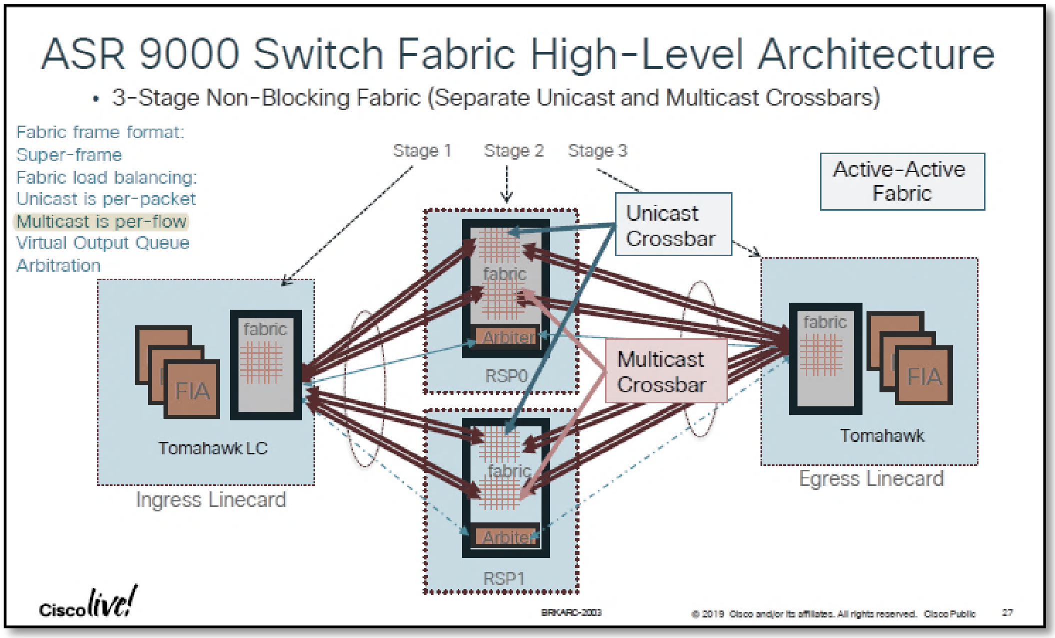
171. One or more of the Cisco ‘209 Products use bidirectional forwarding detection (“BFD”) to determine if an external failure has occurred. An external failure detected through BFD is a Fast Reroute (“FRR”) trigger. The below excerpt from Cisco documentation describes that the Cisco ‘209 Products use FRR which sends a notification to the router “headend.” This notification can be made by the Cisco ‘209 Products through an interior gateway protocol (“IGP”) or through Cisco’s resource reservation protocol (“RSVP”).

> Fast Reroute (FRR) provides link protection to LSPs enabling the traffic carried by LSPs that encounter a failed link to be rerouted around the failure. The reroute decision is controlled locally by the router connected to the failed link. The headend router on the tunnel is notified of the link failure through IGP or through RSVP. When it is notified of a link failure, the headend router attempts to establish a new

> LSP that bypasses the failure. This provides a path to reestablish links that fail, providing protection to data transfer.

MPLS Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 6.5.x at 182 (September 30, 2019).

172. One or more of the Cisco '209 Products include technology for sending, via a first route, a first set of information from an ingress module to a first egress module for forwarding by said first egress module to a destination external to said router, wherein said first set of information traverses a path which encompasses at least a portion of said first route. The following excerpt from a Cisco presentation regarding the Cisco '209 Products shows the process in which a first set of information multicast "per-flow" information is sent from the Ingress Linecard through the fabric and then onto the Egress Linecard.



ASR 9000 Switch Fabric High-Level Architecture

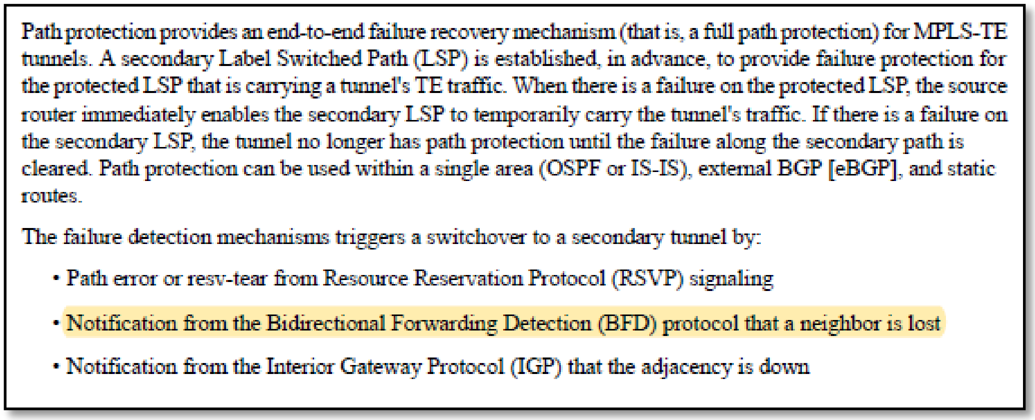
- 3-Stage Non-Blocking Fabric (Separate Unicast and Multicast Crossbars)

Fabric frame format:
Super-frame
Fabric load balancing:
Unicast is per-packet
Multicast is per-flow
Virtual Output Queue
Arbitration

Yongzhong Peng, *Cisco ASR 9000 System Architecture*, Cisco Live Presentation BRKARC-2003 at 27 (2019) (emphasis added).

173. One or more of the Cisco '209 Products include technology for detecting an external failure beyond the first egress module. For example, the Cisco '209 Products include

bidirectional forwarding detection which is a protocol that detects an external failure such as if a "neighbor is lost."



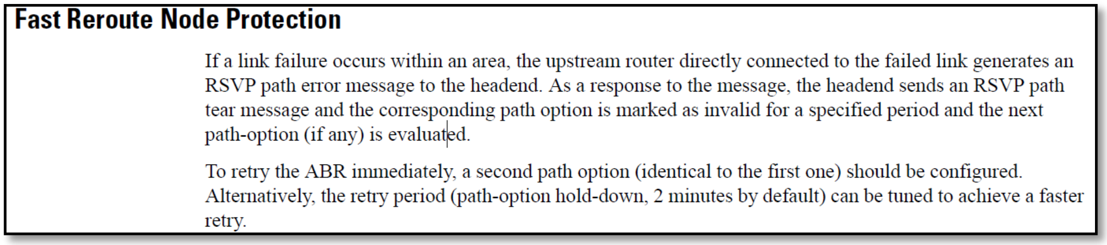
Path protection provides an end-to-end failure recovery mechanism (that is, a full path protection) for MPLS-TE tunnels. A secondary Label Switched Path (LSP) is established, in advance, to provide failure protection for the protected LSP that is carrying a tunnel's TE traffic. When there is a failure on the protected LSP, the source router immediately enables the secondary LSP to temporarily carry the tunnel's traffic. If there is a failure on the secondary LSP, the tunnel no longer has path protection until the failure along the secondary path is cleared. Path protection can be used within a single area (OSPF or IS-IS), external BGP [eBGP], and static routes.

The failure detection mechanisms triggers a switchover to a secondary tunnel by:

- Path error or resv-tear from Resource Reservation Protocol (RSVP) signaling
- Notification from the Bidirectional Forwarding Detection (BFD) protocol that a neighbor is lost
- Notification from the Interior Gateway Protocol (IGP) that the adjacency is down

CISCO ASR 9000 SERIES AGGREGATION SERVICES ROUTER MPLS CONFIGURATION GUIDE, RELEASE 5.3.X at 186 (August 1, 2015) (emphasis added)

174. One or more of the Cisco '209 Products include technology for directing a message to the ingress module informing the ingress module of the external failure in response to the external failure.



Fast Reroute Node Protection

If a link failure occurs within an area, the upstream router directly connected to the failed link generates an RSVP path error message to the headend. As a response to the message, the headend sends an RSVP path tear message and the corresponding path option is marked as invalid for a specified period and the next path-option (if any) is evaluated.

To retry the ABR immediately, a second path option (identical to the first one) should be configured. Alternatively, the retry period (path-option hold-down, 2 minutes by default) can be tuned to achieve a faster retry.

MPLS CONFIGURATION GUIDE FOR CISCO ASR 9000 SERIES ROUTERS, IOS XR RELEASE 6.5.X at 187 (September 30, 2019).

175. One or more of the Cisco '209 Products include technology for selecting an alternate egress module capable of forwarding information to the destination in response to the message.

176. One or more of the Cisco '209 Products include technology for sending, via a second route, a future set of information from the ingress module to the alternate egress module

for forwarding to the destination, wherein the first set of information and the future set of information are both part of a flow.

177. One or more of the Cisco ‘209 Products include technology for causing other sets of information associated with the flow to be sent from the ingress module to the alternate egress module in response to the message.

178. One or more of the Cisco ‘209 Products include technology for directing to the ingress module that comprises: (1) identifying the ingress module; (2) accessing a routing table which comprises one or more routes to the ingress module; (3) obtaining a return route from the routing table, wherein the return route directs the message to the ingress module along a different path than that traversed by said first set of information; and (4) sending a message to the ingress module via the return route.

179. One or more of the Cisco ‘209 Products include technology where the first egress module and the alternate egress module are predetermined, where identifiers associated with the first egress module and the alternate egress module are stored within a flow block associated with the flow. Further, one or more of the Cisco ‘209 Products store an indication in the flow block that all sets of information associated with the flow are to be sent to the alternate egress module.

180. Cisco has directly infringed and continues to directly infringe the ‘209 patent by, among other things, making, using, offering for sale, and/or selling technology for implementing within a network router a method for recovering from a failure, including but not limited to the Cisco ‘209 Products.

181. The Cisco ‘209 Products are available to businesses and individuals throughout the United States.

182. The Cisco '209 Products are provided to businesses and individuals located in the Western District of Texas.

183. By making, using, testing, offering for sale, and/or selling products and services for implementing within a network router a method for recovering from a failure, including but not limited to the Cisco '209 Products, Cisco has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the '209 patent, including at least claim 5 pursuant to 35 U.S.C. § 271(a).

184. Cisco also indirectly infringes the '209 patent by actively inducing infringement under 35 USC § 271(b).

185. Cisco has had knowledge of the '209 patent since at least service of this Complaint or shortly thereafter, and Cisco knew of the '209 patent and knew of its infringement, including by way of this lawsuit.

186. Alternatively, Cisco has had knowledge of the '209 patent since at least September 6, 2007, based on its citation of the '209 patent as relevant prior art in eleven patents and patent applications that are assigned to and owned by Cisco. These patents include:

- U.S. Patent No. 7,940,648 (assigned to Cisco and issued on May 10, 2011).
- U.S. Patent No. 8,116,289 (assigned to Cisco and issued on February 14, 2012).
- U.S. Patent No. 8,432,790 (assigned to Cisco and issued on April 30, 2013).
- U.S. Patent No. 8,543,718 (assigned to Cisco and issued on September 24, 2013).
- U.S. Patent No. 8,966,113 (assigned to Cisco and issued on February 24, 2015).
- U.S. Patent No. 9,300,563 (assigned to Cisco and issued on March 29, 2016).
- U.S. Patent Application No. 2007/0207591 (assigned to Cisco and published on September 6, 2007).
- U.S. Patent Application No. 2007/0208871 (assigned to Cisco and published on September 6, 2007).
- U.S. Patent Application No. 2008/0037419 (assigned to Cisco and published on February 14, 2008).
- U.S. Patent Application No. 2008/0056282 (assigned to Cisco and published on March 6, 2008).
- U.S. Patent Application No. 2011/0141880 (assigned to Cisco and published on June 16, 2011).

187. Cisco intended to induce patent infringement by third-party customers and users of the Cisco '209 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the '209 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '209 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco '209 Products that have the capability of operating in a manner that infringe one or more of the claims of the '209 patent, including at least claim 5, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '209 Products to utilize the products in a manner that directly infringe one or more claims of the '209 patent.[25] By providing instruction and training to customers and end-users on how to use the Cisco '209 Products in a manner that directly infringes one or more claims of the '209 patent, including at least claim 5, Cisco specifically intended to induce infringement of the '209 patent. Cisco engaged in such inducement to promote the sales of the Cisco '209 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '209 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '209 patent, knowing that such use constitutes infringement of the '209 patent.

[25] *See, e.g.,* Sabyasachi Kar & Shashi Shekhar Sharma, *Next Generation Multicast VPN & Advanced Design,* CISCO LIVE PRESENTATION LTRMPL-3103 (2017); CISCO ASR 9000 SERIES AGGREGATION SERVICES ROUTER MPLS CONFIGURATION GUIDE, RELEASE 5.3.X (August 1, 2015); CISCO ASR 9000 SERIES AGGREGATION SERVICES ROUTER ROUTING CONFIGURATION GUIDE, RELEASE 6.1.X (November 2, 2016); MPLS CONFIGURATION GUIDE FOR CISCO ASR 9000 SERIES ROUTERS, IOS XR RELEASE 6.5.X (September 30, 2019); *ASR 9000 Operation & Troubleshooting,* CISCO LIVE PRESENTATION TECSPG-3001 (2015); and CISCO IOS SOFTWARE CONFIGURATION GUIDE, RELEASE 15.0SY: MPLS QOS (January 19, 2018).

188. The ‘209 patent is well-known within the industry as demonstrated by multiple citations to the ‘209 patent in published patents and patent applications assigned to technology companies and academic institutions. Cisco is utilizing the technology claimed in the ‘209 patent without paying a reasonable royalty. Cisco is infringing the ‘209 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

189. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘209 patent.

190. As a result of Cisco’s infringement of the ‘209 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Cisco’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 8,085,775

191. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

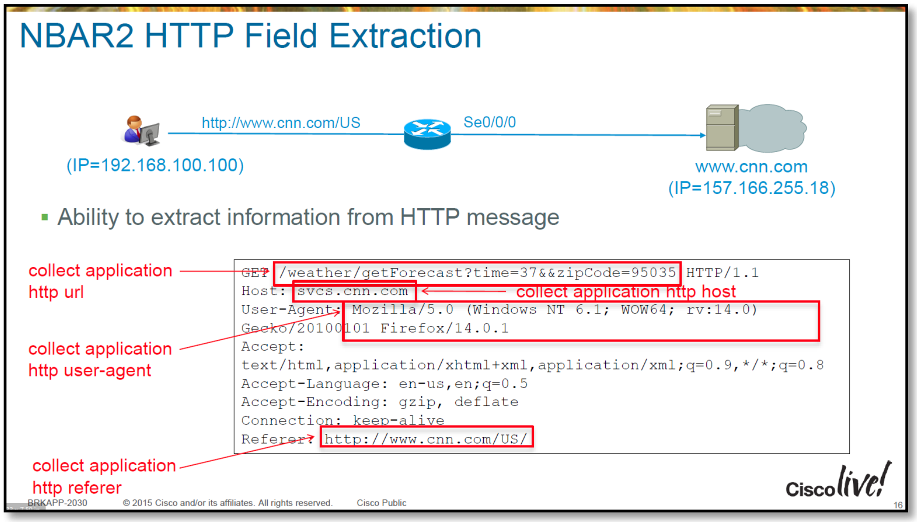
192. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for identifying and handling a single application flow of a plurality of information packets.

193. Cisco designs, makes, sells, offers to sell, imports, and/or uses routers containing Cisco’s Application Visibility and Control functionality, including at least the following routers: Cisco 800 Series Industrial Integrated Services Routers, Cisco 900 Series Industrial Routers, Cisco 900 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, Cisco 4000

Series Integrated Services Routers, Cisco Cloud Services Router 1000V Series, and Cisco ASR 1000 Series Aggregation Services Routers (collectively, the "Cisco '775 Products(s)").

194. One or more Cisco subsidiaries and/or affiliates use the Cisco '775 Products in regular business operations.

195. One or more of the Cisco '775 Products include technology for identifying and handling a single application flow of a plurality of information packets. For example, the Cisco '775 Products contain functionality for extracting information from an HTTP packet to identify an application flow.



NBAR2 HTTP Field Extraction

- Ability to extract information from HTTP message

```
GET /weather/getForecast?time=37&&zipCode=95035 HTTP/1.1
Host: svcs.cnn.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.cnn.com/US/
```

collect application http url
collect application http host
collect application http user-agent
collect application http referer
Cisco live!

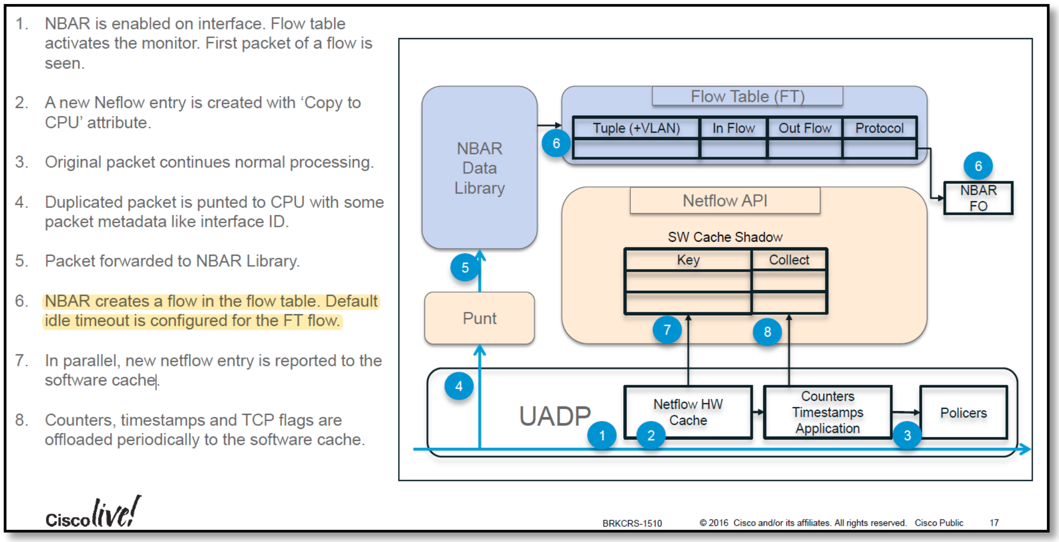
BRKAPP-2030 © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public 16

Karthik Dakshinamoorthy, *Application Visibility and Control in Enterprise WAN Application Visibility, Monitoring, Troubleshooting & Manageability,* CISCO LIVE PRESENTATION BRKAPP-2030 at 16 (2015).

196. Cisco has directly infringed and continues to directly infringe the '775 patent by, among other things, making, using, offering for sale, and/or selling technology for identifying and handling a single application flow of a plurality of information packets, including but not limited to the Cisco '775 Products.

197. One or more of the Cisco '775 Products creates a flow block as the first packet of a flow is processed by a router. The following except from a Cisco presentation shows the

functionality for the Cisco '775 Products creating a "Flow Table" when the first packet of a flow is processed.



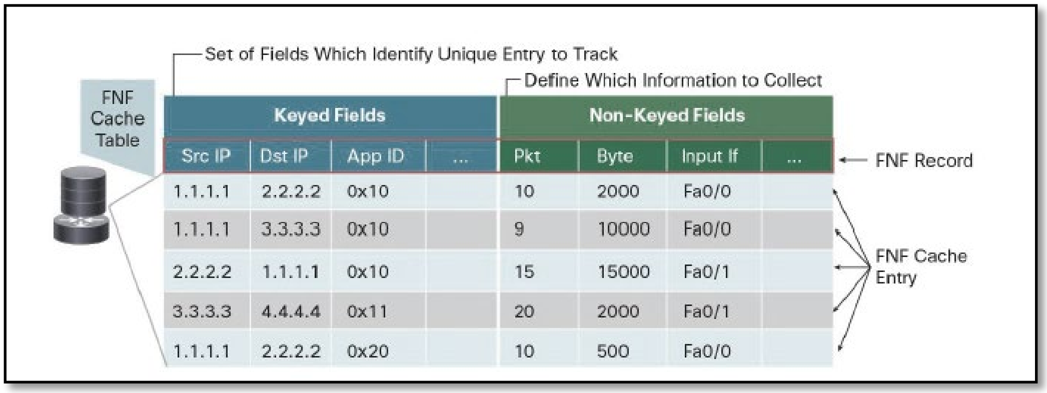
1. NBAR is enabled on interface. Flow table activates the monitor. First packet of a flow is seen.
2. A new Neflow entry is created with 'Copy to CPU' attribute.
3. Original packet continues normal processing.
4. Duplicated packet is punted to CPU with some packet metadata like interface ID.
5. Packet forwarded to NBAR Library.
6. NBAR creates a flow in the flow table. Default idle timeout is configured for the FT flow.
7. In parallel, new netflow entry is reported to the software cache.
8. Counters, timestamps and TCP flags are offloaded periodically to the software cache.

Cisco live!

BRKCRS-1510 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public 17

Tarunesh Ahuja, *Prioritize Applications with Application Visibility and Control in Campus Network*, CISCO LIVE PRESENTATION BRKCRS-1510 rat 17 (2016) (emphasis added).

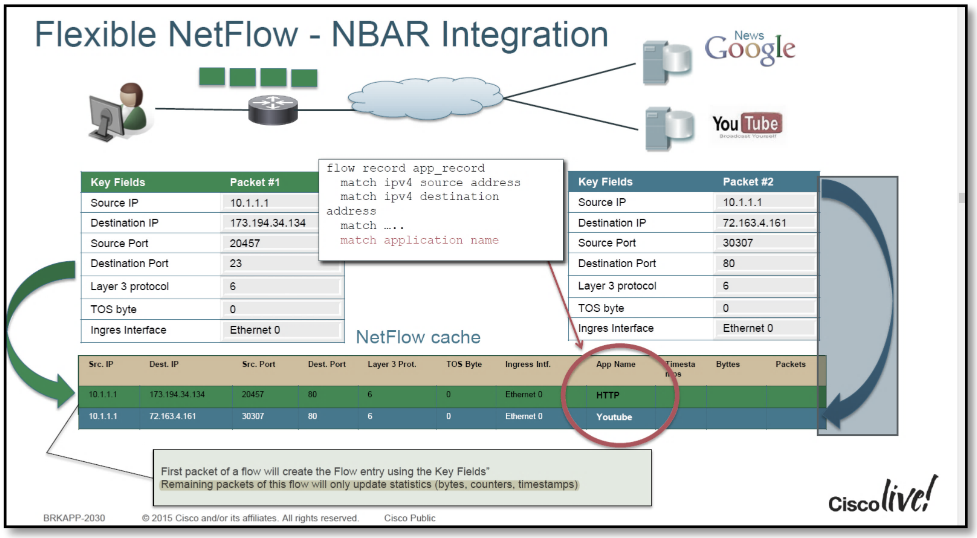
198. One or more of the Cisco '775 Products utilize a flow block adapted to store payload-content agnostic behavioral statistics about the flow. For example, the Cisco '775 products generate flow based identifiers for the packets based on fields that are no with the payload of the packet. The below excerpt from a Cisco presentation on Cisco's Application Visibility and Control ("AVC") functionality shows that the information collected and export to AVC is based on traffic flow information and application statistics such as byte and packet count.


Set of Fields Which Identify Unique Entry to Track
Define Which Information to Collect
FNF Cache Table
FNF Record
FNF Cache Entry

Keyed Fields				Non-Keyed Fields			
Src IP	Dst IP	App ID	...	Pkt	Byte	Input If	...
1.1.1.1	2.2.2.2	0x10		10	2000	Fa0/0	
1.1.1.1	3.3.3.3	0x10		9	10000	Fa0/0	
2.2.2.2	1.1.1.1	0x10		15	15000	Fa0/1	
3.3.3.3	4.4.4.4	0x11		20	2000	Fa0/1	
1.1.1.1	2.2.2.2	0x20		10	500	Fa0/0	

AVC Solution Guide with Cisco Prime Infrastructure, CISCO SOLUTION OVERVIEW at 8 (2015).

199. One or more of the Cisco '775 Products update the flow block with the flow's payload-content agnostic behavioral statistics as packets belonging to the flow are processed by the router. For example, the payload-content agnostic behavioral statistics that are calculated by the Cisco '775 Products include the total byte count accumulated for the flow which is shown in the below excerpt from Cisco's documentation of the Cisco '775 Products.


Flexible NetFlow - NBAR Integration

Key Fields	Packet #1
Source IP	10.1.1.1
Destination IP	173.194.34.134
Source Port	20457
Destination Port	23
Layer 3 protocol	6
TOS byte	0
Ingres Interface	Ethernet 0

```
flow record app_record
  match ipv4 source address
  match ipv4 destination
address
  match …..
  match application name
```

Key Fields	Packet #2
Source IP	10.1.1.1
Destination IP	72.163.4.161
Source Port	30307
Destination Port	80
Layer 3 protocol	6
TOS byte	0
Ingres Interface	Ethernet 0

Src. IP	Dest. IP	Src. Port	Dest. Port	Layer 3 Prot.	TOS Byte	Ingress Intf.	App Name	Timestamps	Bytes	Packets
10.1.1.1	173.194.34.134	20457	80	6	0	Ethernet 0	HTTP			
10.1.1.1	72.163.4.161	30307	80	6	0	Ethernet 0	Youtube			

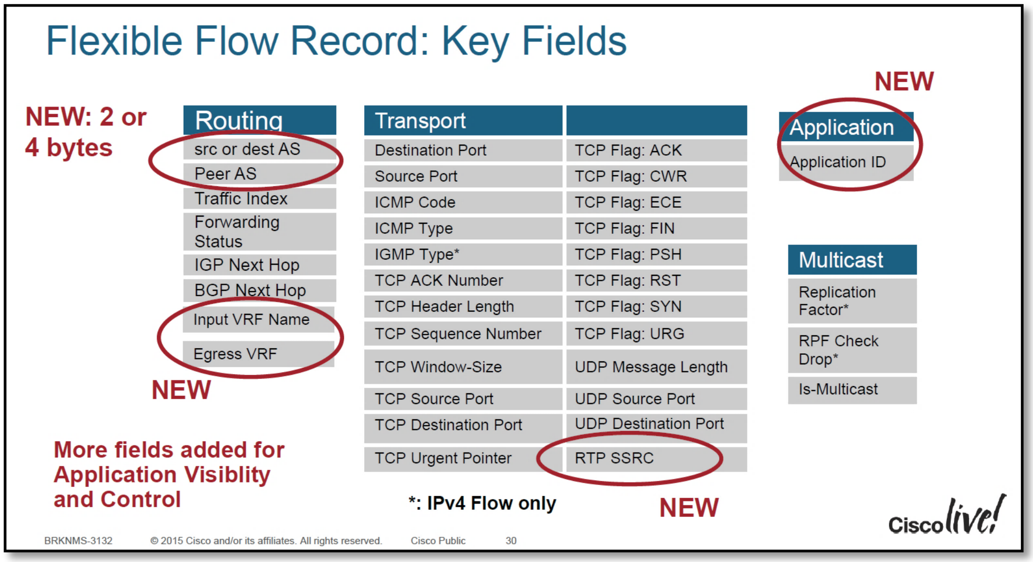
First packet of a flow will create the Flow entry using the Key Fields"
Remaining packets of this flow will only update statistics (bytes, counters, timestamps)

BRKAPP-2030 © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Karthik Dakshinamoorthy, *Application Visibility and Control in Enterprise WAN Application Visibility, Monitoring, Troubleshooting & Manageability,* CISCO LIVE PRESENTATION BRKAPP-2030 at 48 (2015).

200. One or more of the Cisco '775 Products utilize a flow incapable of being identified by header information alone. For example, the below Flexible Flow Record used by Cisco AVC

shows the flow cannot be identified by header information alone. Instead, the identity of the flow must be processed using a heuristic analysis to identify the identity of the flow (the application type of the flow).



Flexible Flow Record: Key Fields

NEW: 2 or 4 bytes

Routing
src or dest AS
Peer AS
Traffic Index
Forwarding Status
IGP Next Hop
BGP Next Hop
Input VRF Name
Egress VRF

NEW

More fields added for Application Visiblity and Control

Transport	
Destination Port	TCP Flag: ACK
Source Port	TCP Flag: CWR
ICMP Code	TCP Flag: ECE
ICMP Type	TCP Flag: FIN
IGMP Type*	TCP Flag: PSH
TCP ACK Number	TCP Flag: RST
TCP Header Length	TCP Flag: SYN
TCP Sequence Number	TCP Flag: URG
TCP Window-Size	UDP Message Length
TCP Source Port	UDP Source Port
TCP Destination Port	UDP Destination Port
TCP Urgent Pointer	RTP SSRC

*: IPv4 Flow only

NEW

NEW

Application
Application ID

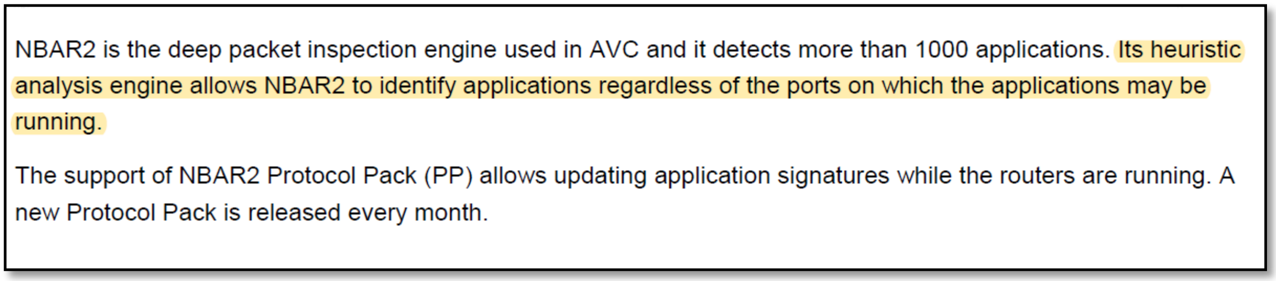
Multicast
Replication Factor*
RPF Check Drop*
Is-Multicast

Cisco live!

BRKNMS-3132 © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public 30

Benoit Claise, *Advanced NetFlow*, CISCO LIVE PRESENTATION BRKNMS-3132 at 30 (2015).

201. One or more of the Cisco '775 Products heuristically determine whether at least one user-specified policy is satisfied by the payload-content agnostic behavioral statistics stored in the flow block. For example, the Cisco '775 Products use a heuristic analysis to identify applications regardless of the ports on which the applications may be running. This process is described in the below excerpt from Cisco's documentation of the '775 Products.

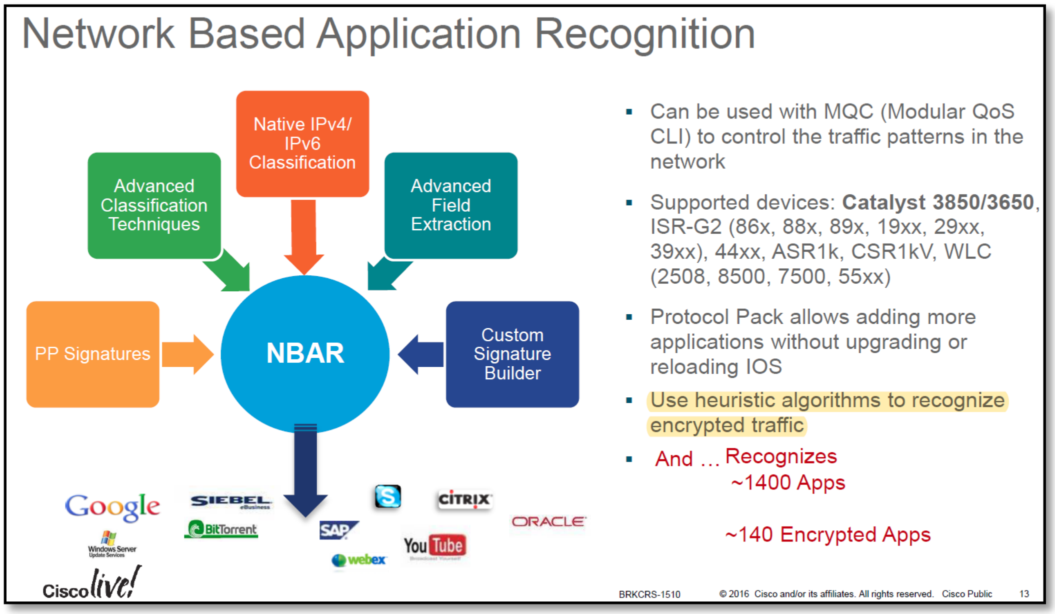


NBAR2 is the deep packet inspection engine used in AVC and it detects more than 1000 applications. Its heuristic analysis engine allows NBAR2 to identify applications regardless of the ports on which the applications may be running.

The support of NBAR2 Protocol Pack (PP) allows updating application signatures while the routers are running. A new Protocol Pack is released every month.

AVC Solution Guide with Cisco Prime Infrastructure, CISCO SOLUTION OVERVIEW at 10 (2015) (emphasis added).

202. The Cisco '775 Products can heuristically determine whether at least one user-specified policy is satisfied by said payload-content agnostic behavioral statistics stored in a flow block where the flow payload is encrypted. For example, when a web-based application is opened in a browser, the browser first communicates with a DNS server to request the IP address of the relevant server for the application. The DNS transaction consists of a request and response; the response contains the IP address of the server for the web-based application. This payload content agnostic behavioral information is stored in the flow block. The Cisco '775 Products then contain functionality to use this information to correctly associate the web-based application with the relevant server IP address. The Cisco '775 Products can then identify future traffic involving that IP address from the first packet of the flow. The below excerpt from a Cisco presentation on the Cisco '775 Products substantiates the heuristic determination of a flow identity based on payload-content agnostic behavior.


Native IPv4/ IPv6 Classification
Advanced Classification Techniques
Advanced Field Extraction
PP Signatures
NBAR
Custom Signature Builder
Google
SIEBEL eBusiness
BitTorrent
Windows Server Update Services
SAP
webex
CITRIX
YouTube
ORACLE
Cisco live!

Network Based Application Recognition

- Can be used with MQC (Modular QoS CLI) to control the traffic patterns in the network
- Supported devices: **Catalyst 3850/3650**, ISR-G2 (86x, 88x, 89x, 19xx, 29xx, 39xx), 44xx, ASR1k, CSR1kV, WLC (2508, 8500, 7500, 55xx)
- Protocol Pack allows adding more applications without upgrading or reloading IOS
- Use heuristic algorithms to recognize encrypted traffic
- And … Recognizes ~1400 Apps

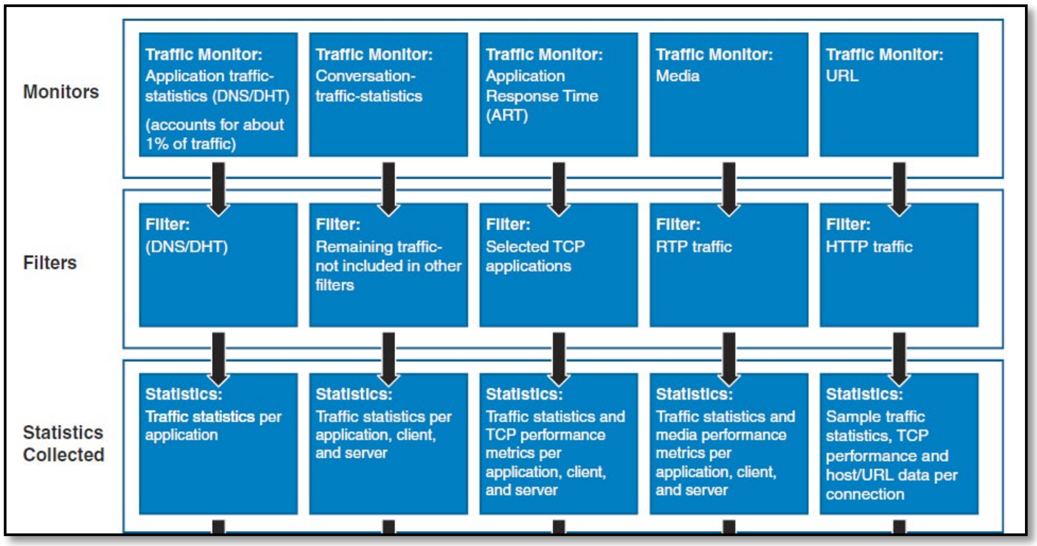
~140 Encrypted Apps

BRKCRS-1510 © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public 13

Tarunesh Ahuja, *Prioritize Applications with Application Visibility and Control in Campus Network*, CISCO LIVE PRESENTATION BRKCRS-1510 at 13 (2016) (emphasis added).

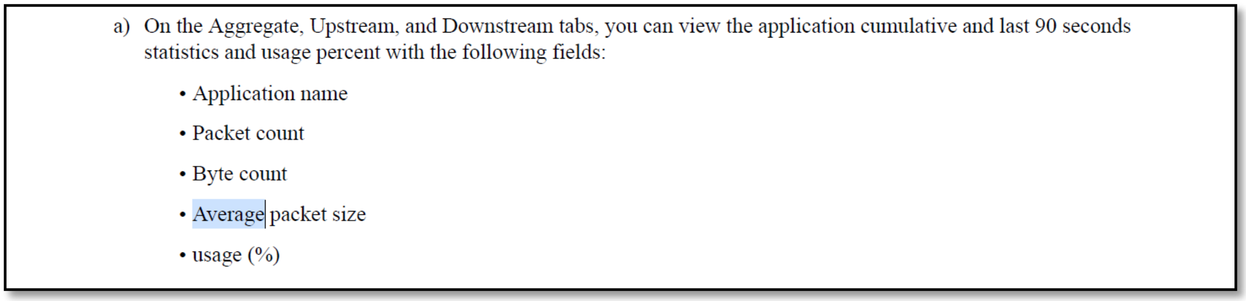
203. One or more of the Cisco '775 Products apply to at least one packet belonging to at least one user-specified action that is mapped to the user-specified policy that is satisfied by the payload-content agnostic behavioral statistics upon determining that the user-specified policy is satisfied by the payload-content agnostic behavioral statistics.

204. One or more of the Cisco '775 Products include functionality wherein the payload-content agnostic behavioral statistics for the flow are calculated by the router. The below excerpt from a Cisco user guide for the Cisco '775 Product shows one instance where the behavioral statistics are calculated by a router.


Monitors
Filters
Statistics Collected
Traffic Monitor: Application traffic-statistics (DNS/DHT) (accounts for about 1% of traffic)
Traffic Monitor: Conversation-traffic-statistics
Traffic Monitor: Application Response Time (ART)
Traffic Monitor: Media
Traffic Monitor: URL
Filter: (DNS/DHT)
Filter: Remaining traffic-not included in other filters
Filter: Selected TCP applications
Filter: RTP traffic
Filter: HTTP traffic
Statistics: Traffic statistics per application
Statistics: Traffic statistics per application, client, and server
Statistics: Traffic statistics and TCP performance metrics per application, client, and server
Statistics: Traffic statistics and media performance metrics per application, client, and server
Statistics: Sample traffic statistics, TCP performance and host/URL data per connection

CISCO APPLICATION VISIBILITY AND CONTROL USER GUIDE at 4-7 (December 2018).

205. One or more of the Cisco '775 Products include functionality wherein the payload-content agnostic behavioral statistics reflect the empirical behavior of the flow. The below excerpt from Cisco documentation shows that the statistics calculated by the Cisco '775 Products include empirical behavior such as "packet count," "byte count," and "average packet size."



a) On the Aggregate, Upstream, and Downstream tabs, you can view the application cumulative and last 90 seconds statistics and usage percent with the following fields:

- Application name
- Packet count
- Byte count
- Average packet size
- usage (%)

CONSOLIDATED PLATFORM CONFIGURATION GUIDE, CISCO IOS XE 3.3SE at 10 (2013) (emphasis added).

206. One or more of the Cisco ‘775 Products include functionality wherein at least one of the payload-content agnostic behavioral statistics is chosen from the group consisting of: (1) total byte count accumulated for the flow, (2) flow life duration, (3) average rate of flow, (4) average packet size, (5) average packet rate, (6) average inter-packet gap, (7) instantaneous flow rate, and (8) moving average flow rate.

207. The Cisco ‘775 Products are available to businesses and individuals throughout the United States.

208. The Cisco ‘775 Products are provided to businesses and individuals located in the Western District of Texas.

209. By making, using, testing, offering for sale, and/or selling products and services for identifying and handling a single application flow of a plurality of information packets, including but not limited to the Cisco ‘775 Products, Cisco has injured Plaintiffs and is liable to Plaintiffs for directly infringing one or more claims of the ‘775 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

210. Cisco also indirectly infringes the ‘775 patent by actively inducing infringement under 35 USC § 271(b).

211. Cisco has had knowledge of the ‘775 patent since at least service of this Complaint or shortly thereafter, and Cisco knew of the ‘775 patent and knew of its infringement, including by way of this lawsuit.

212. Alternatively, Cisco has had knowledge of the ‘775 patent since at least January 22, 2015, based on its citation of the ‘775 patent as relevant prior art in four patents and patent applications that are assigned to and owned by Cisco. These patents include:

- U.S, Patent No. 9,680,760 (assigned to Cisco and issued on June 13, 2017).
- U.S. Patent No. 10,103,991 (assigned to Cisco and issued on October 16, 2018).
- U.S. Patent Application No. 2015/0023366 (assigned to Cisco and published on January 22, 2015).
- U.S. Patent Application. No. 2016/0112323 (assigned to Cisco and published on April 21, 2016).

213. Cisco intended to induce patent infringement by third-party customers and users of the Cisco ‘775 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘775 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘775 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco ‘775 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘775 patent, including at least claim 1, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco ‘775 Products to utilize the products in a manner that directly infringe one or more claims of the ‘775 patent.[26] By providing

[26] *See, e.g.,* Karthik Dakshinamoorthy, *Application Visibility and Control in Enterprise WAN Application Visibility, Monitoring, Troubleshooting & Manageability*, CISCO LIVE PRESENTATION BRKAPP-2030 (2015); Benoit Claise, *Advanced NetFlow,* CISCO LIVE PRESENTATION BRKNMS-3132 (2015); Tarunesh Ahuja, *Prioritize Applications with Application Visibility and Control in Campus Network*, CISCO LIVE PRESENTATION BRKCRS-

instruction and training to customers and end-users on how to use the Cisco '775 Products in a manner that directly infringes one or more claims of the '775 patent, including at least claim 1, Cisco specifically intended to induce infringement of the '775 patent. Cisco engaged in such inducement to promote the sales of the Cisco '775 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '775 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '775 patent, knowing that such use constitutes infringement of the '775 patent.

214. The '775 patent is well-known within the industry as demonstrated by multiple citations to the '775 patent in published patents and patent applications assigned to technology companies and academic institutions. Cisco is utilizing the technology claimed in the '775 patent without paying a reasonable royalty. Cisco is infringing the '775 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

215. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '775 patent.

216. As a result of Cisco's infringement of the '775 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

1510 (2016); *AVC Solution Guide with Cisco Prime Infrastructure*, CISCO SOLUTION OVERVIEW (2015); *AVC Solution Guide with Cisco Prime Infrastructure*, CISCO SOLUTION OVERVIEW (2015); *Application Monitoring Using Net Flow*, CISCO TECHNOLOGY DESIGN GUIDE (December 2013); CISCO APPLICATION VISIBILITY AND CONTROL USER GUIDE (December 2018); and CONSOLIDATED PLATFORM CONFIGURATION GUIDE, CISCO IOS XE 3.3SE (CATALYST 3850 SWITCHES) (2013).

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 8,817,790

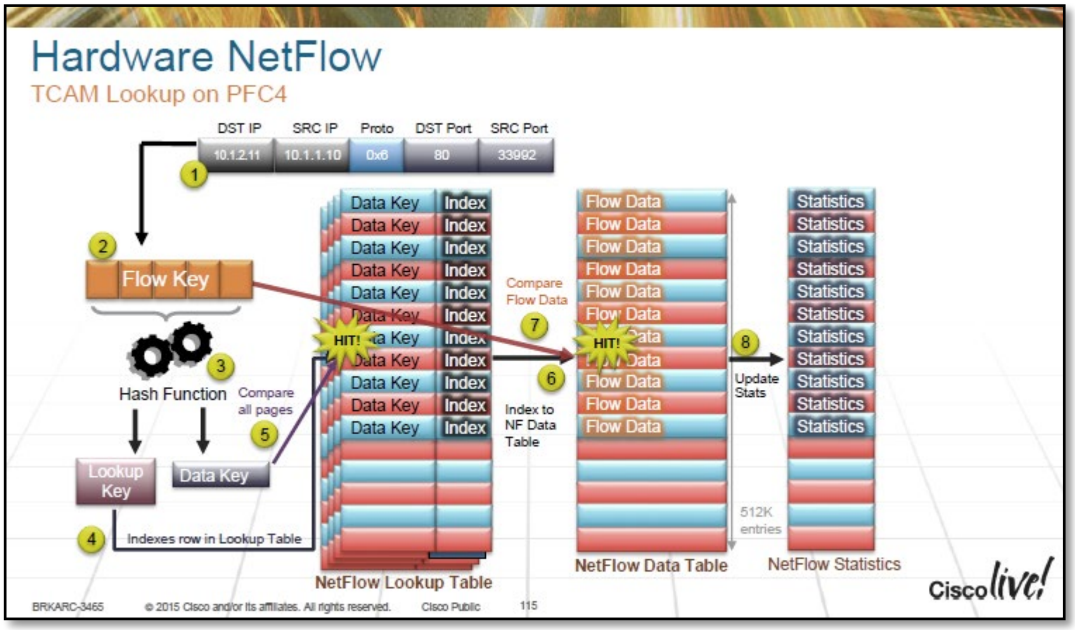
217. Plaintiffs reference and incorporate by reference the preceding paragraphs of this Complaint as if fully set forth herein.

218. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for handling a flow of information packets.

219. Cisco designs, makes, sells, offers to sell, imports, and/or uses routers containing Cisco's Application Visibility and Control functionality including at least the following routers: Cisco 800 Series Industrial Integrated Services Routers, Cisco 900 Series Industrial Routers, Cisco 900 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, Cisco 4000 Series Integrated Services Routers, Cisco Cloud Services Router 1000V Series, and Cisco ASR 1000 Series Aggregation Services Routers (collectively, the "Cisco '790 Products(s)").

220. One or more Cisco subsidiaries and/or affiliates use the Cisco '790 Products in regular business operations.

221. One or more of the Cisco '790 Products include technology for handling a flow of information packets. Specifically, the Cisco '790 Product process information packets that have the same header information. In the below excerpt from Cisco documentation, the header information is generated into a "Flow Key" that is then compared in the "Lookup Table" to determine if another information packet had the same header information. If so a match is identified and the incoming information packet is assigned to the flow that has the matching header.



Hardware NetFlow

TCAM Lookup on PFC4

BRKARC-3465 © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public 115

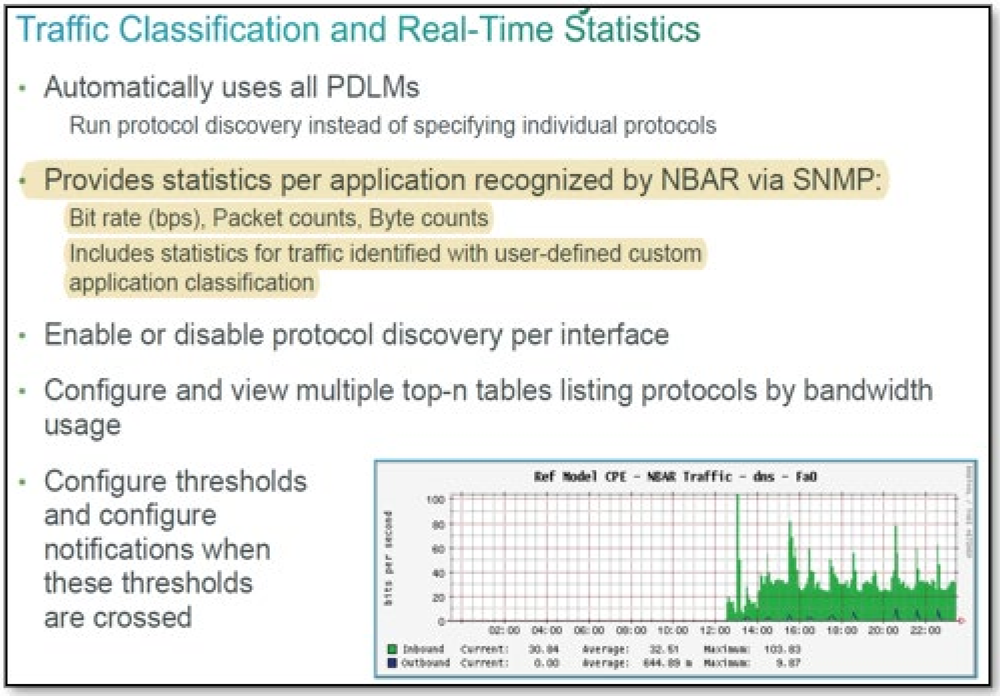
Shawn Wargo, *Catalyst 6800 Switch Architectures*, CISCO LIVE PRESENTATION BRKARC-3465 at 115 (2015).

222. The Cisco '790 Products are available to businesses and individuals throughout the United States.

223. The Cisco '790 Products are provided to businesses and individuals located in the Western District of Texas.

224. Cisco has directly infringed and continues to directly infringe the '790 patent by, among other things, making, using, offering for sale, and/or selling technology for handling a flow of information packets, including but not limited to the Cisco '790 Products.

225. The Cisco '790 Products process a flow comprised of two or more information packets having header information in common. Further, the Cisco '790 Products use header-independent statistics for traffic classification. These statistics include bit rate, packet counts, and byte counts that are used to identify a particular traffic type. The following excerpt from Cisco documentation for the Cisco '790 Products shows the ability to conduct traffic classification based on statistics that are header-independent.



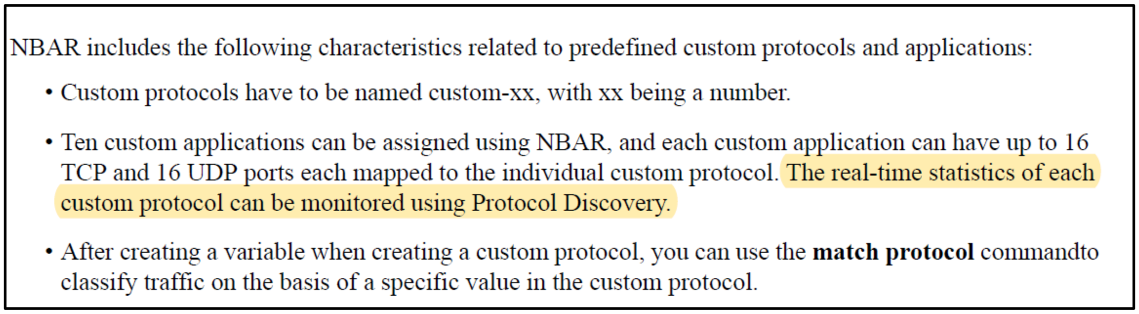
Traffic Classification and Real-Time Statistics

- Automatically uses all PDLMs
  Run protocol discovery instead of specifying individual protocols
- Provides statistics per application recognized by NBAR via SNMP:
  Bit rate (bps), Packet counts, Byte counts
  Includes statistics for traffic identified with user-defined custom application classification
- Enable or disable protocol discovery per interface
- Configure and view multiple top-n tables listing protocols by bandwidth usage
- Configure thresholds and configure notifications when these thresholds are crossed

Ref Model CPE - NBAR Traffic - dns - Fa0
bits per second
100
80
60
40
20
0
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
🟩 Inbound Current: 30.84 Average: 32.51 Maximum: 103.83
🟦 Outbound Current: 0.00 Average: 644.89 m Maximum: 9.87

Chris Hocker, *Innovations and Approaches to Traffic Flow Management*, CISCO LIVE PRESENTATION at 47 (2012).

226. The Cisco ‘790 Products store header-independent statistics about the flow in a flow block associated with the flow. Specifically, each time a packet is processed by the Cisco ‘790 Products, the header-independent data can stored in the NetFlow Data Table and the statistics for the flow are updated. Further, the NBAR Protocol Discovery MIB enables the use of per interface, per protocol and bi-directional statistics (bit rate (bps), packet counts and byte counts) to conduct traffic identification and matching for packets.

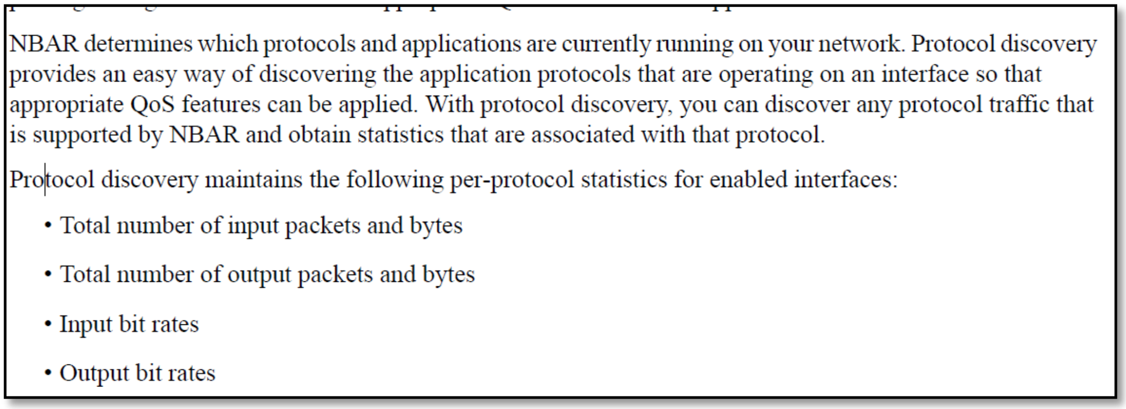


NBAR includes the following characteristics related to predefined custom protocols and applications:

- Custom protocols have to be named custom-xx, with xx being a number.
- Ten custom applications can be assigned using NBAR, and each custom application can have up to 16 TCP and 16 UDP ports each mapped to the individual custom protocol. The real-time statistics of each custom protocol can be monitored using Protocol Discovery.
- After creating a variable when creating a custom protocol, you can use the **match protocol** commandto classify traffic on the basis of a specific value in the custom protocol.

QOS: NBAR CONFIGURATION GUIDE at 11 (March 22, 2018) (emphasis added).

227. The Cisco '790 Products perform traffic matching using header-independent statistics such as: total number of input packets, total number of output packets, input bit rates, and output bit rates. The following excerpt from Cisco documentation of the Cisco '790 Products shows the use of these header-independent statistics to perform traffic matching.



NBAR determines which protocols and applications are currently running on your network. Protocol discovery provides an easy way of discovering the application protocols that are operating on an interface so that appropriate QoS features can be applied. With protocol discovery, you can discover any protocol traffic that is supported by NBAR and obtain statistics that are associated with that protocol.

Protocol discovery maintains the following per-protocol statistics for enabled interfaces:

- Total number of input packets and bytes
- Total number of output packets and bytes
- Input bit rates
- Output bit rates

QOS: NBAR CONFIGURATION GUIDE at 53 (March 22, 2018) (emphasis added).

228. The Cisco '790 Products apply traffic policies to one or more information packets belonging to traffic types that are designated as matching a particular traffic type by the user. "Traffic that matches a user-specified criterion can be organized into specific classes. The traffic in those classes can, in turn, receive specific QoS treatment when that class is included in a policy map."[27]

[27] QOS: NBAR CONFIGURATION GUIDE at 122 (March 22, 2018) (emphasis added).

229. The Cisco '790 Products use statistics that are generated by the Cisco '790 Products to define classes and traffic policies (sometimes referred to as policy maps by Cisco) for each traffic class. "The traffic policies (policy maps) are used to apply specific QoS features and functionality to the traffic classes."[28]

230. The Cisco '790 Products update the header-independent statistics in the flow block as each information packet belonging to the flow is processed. The header-independent statistics are stored in a flow block associated with the flow. Further, the header-independent information is stored in a flow block that is associated with the flow. This data is identified as the "NetFlow Statistics" and can be stored by the Cisco '790 Products in the "Netflow Data Table."

231. The Cisco '790 Products categorize the flow as one or more traffic types by determining whether the header-independent statistics match one or more profiles corresponding to a traffic type. The Cisco '790 Products categorize a flow as a traffic type (e.g., the flow is associated with an application) using header independent statistics such as "average rate," "average packet size," "total byte count," "duration of the flow," "flow rate," etc. The following tables show some of the header-independent statists that are used to match a flow to a corresponding traffic type.

[28] *Id*. at 53.

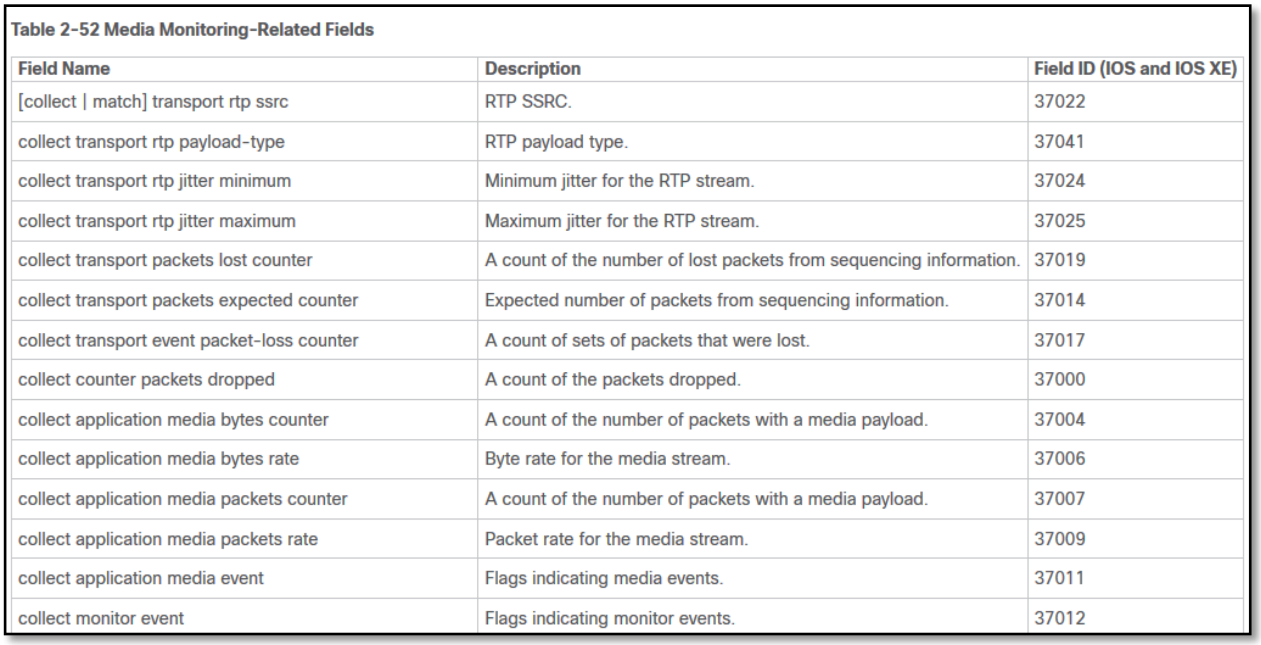


Table 2-52 Media Monitoring-Related Fields

Field Name	Description	Field ID (IOS and IOS XE)
[collect | match] transport rtp ssrc	RTP SSRC.	37022
collect transport rtp payload-type	RTP payload type.	37041
collect transport rtp jitter minimum	Minimum jitter for the RTP stream.	37024
collect transport rtp jitter maximum	Maximum jitter for the RTP stream.	37025
collect transport packets lost counter	A count of the number of lost packets from sequencing information.	37019
collect transport packets expected counter	Expected number of packets from sequencing information.	37014
collect transport event packet-loss counter	A count of sets of packets that were lost.	37017
collect counter packets dropped	A count of the packets dropped.	37000
collect application media bytes counter	A count of the number of packets with a media payload.	37004
collect application media bytes rate	Byte rate for the media stream.	37006
collect application media packets counter	A count of the number of packets with a media payload.	37007
collect application media packets rate	Packet rate for the media stream.	37009
collect application media event	Flags indicating media events.	37011
collect monitor event	Flags indicating monitor events.	37012

Cisco Application Visibility and Control Field Definition Guide for Third-Party Customers at 2-33 (November 29, 2017).

232. The Cisco ‘790 Products perform an operation that is determined according to the one or more traffic types on one or more information packets belonging to the flow if the one or more traffic types match one or more particular traffic types designated by a user.

233. By making, using, testing, offering for sale, and/or selling products and services, including but not limited to the Cisco ‘790 Products, Cisco has injured Plaintiffs and is liable for directly infringing one or more claims of the ‘790 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

234. Cisco also indirectly infringes the ‘790 patent by actively inducing infringement under 35 USC § 271(b).

235. Cisco has had knowledge of the ‘790 patent since at least service of this Complaint or shortly thereafter, and Cisco knew of the ‘790 patent and knew of its infringement, including by way of this lawsuit.

236. Alternatively, Cisco has had knowledge of the ‘790 patent since at least January 22, 2015, based on its citation of the ‘790 patent application as relevant prior two patents and patent applications that are assigned to and owned by Cisco. These patents include:

- U.S, Patent No. 9,680,760 (assigned to Cisco and issued on June 13, 2017).
- U.S. Patent Application No. 2015/0023366 (assigned to Cisco and published on January 22, 2015).

237. Cisco intended to induce patent infringement by third-party customers and users of the Cisco ‘790 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘790 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘790 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco ‘790 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘790 patent, including at least claim 1, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco ‘790 Products to utilize the products in a manner that directly infringe one or more claims of the ‘790 patent.29 By providing instruction and training to customers and end-users on how to use the Cisco ‘790 Products in a

[29] *See, e.g.,* Karthik Dakshinamoorthy, *Application Visibility and Control in Enterprise WAN Application Visibility, Monitoring, Troubleshooting & Manageability*, CISCO LIVE PRESENTATION BRKAPP-2030 (2015); Benoit Claise, *Advanced NetFlow,* CISCO LIVE PRESENTATION BRKNMS-3132 (2015); Tarunesh Ahuja, *Prioritize Applications with Application Visibility and Control in Campus Network*, CISCO LIVE PRESENTATION BRKCRS-1510 (2016); *AVC Solution Guide with Cisco Prime Infrastructure*, CISCO SOLUTION OVERVIEW (2015); *AVC Solution Guide with Cisco Prime Infrastructure*, CISCO SOLUTION OVERVIEW (2015); *Application Monitoring Using Net Flow*, CISCO TECHNOLOGY DESIGN GUIDE (December 2013); CISCO APPLICATION VISIBILITY AND CONTROL USER GUIDE (December 2018); and CONSOLIDATED PLATFORM CONFIGURATION GUIDE, CISCO IOS XE 3.3SE (CATALYST 3850 SWITCHES) (2013).

manner that directly infringes one or more claims of the ‘790 patent, including at least claim 1, Cisco specifically intended to induce infringement of the ‘790 patent. Cisco engaged in such inducement to promote the sales of the Cisco ‘790 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘790 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘790 patent, knowing that such use constitutes infringement of the ‘790 patent.

238. The ‘790 patent is well-known within the industry as demonstrated by multiple citations to the ‘790 patent in published patents and patent applications assigned to technology companies and academic institutions. Cisco is utilizing the technology claimed in the ‘790 patent without paying a reasonable royalty. Cisco is infringing the ‘790 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

239. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘790 patent.

240. As a result of Cisco’s infringement of the ‘790 patent, Plaintiffs have suffered monetary damages, and seek recovery in an amount adequate to compensate for Cisco’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Sable IP, LLC and Sable Networks, Inc. respectfully request that this Court enter:

A. A judgment in favor of Plaintiffs that Cisco has infringed, either literally and/or under the doctrine of equivalents, the '431, '932, '919, '209, '775, and '790 patents;

B. An award of damages resulting from Cisco's acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order finding that Cisco's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiffs enhanced damages.

D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiffs their reasonable attorneys' fees against Cisco.

E. Any and all other relief to which Plaintiffs may show themselves to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Sable IP, LLC and Sable Networks, Inc. request a trial by jury of any issues so triable by right.

Dated: April 13, 2020

Respectfully submitted,

/s/ Daniel P. Hipskind
Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
Eric B. Hanson (CA SB No. 254570)
BERGER & HIPSKIND LLP
9538 Brighton Way, Ste. 320
Beverly Hills, CA 90210
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com
E-mail: ebh@bergerhipskind.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP
114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com

Attorneys for Sable Networks, Inc. and Sable IP, LLC